uc3m | Universidad Carlos III de Madrid

Grado Universitario Ingeniería en Tecnologías de Telecomunicación.

2017-2018

Trabajo Fin de Grado

"Inhibición de señales GSM en Software Defined Radio"

Álvaro Rojo Ortego

Tutor/es

Víctor Pedro Gil Jiménez

Leganés, 2018

RESUMEN

En este proyecto vamos a implementar un inhibidor de frecuencias de la red GSM en tecnología SDR. Esta tecnología es elegida por su alta capacidad de actualización al estar definida por software, lo cual posibilita su uso para varias redes a la vez.

La inhibición consiste en bloquear la comunicación entre el terminal móvil y la estación base, para que no se sincronice con esta última. Esto se consigue gracias al uso de señales iguales a las señales de sincronización utilizadas por la estación base de la red GSM con la diferencia de que las nuestras solo llevan ruido, es decir, no contienen información de sincronización. De esta manera, atacando a los canales de control que manda la estación base por el enlace de bajada, el terminal móvil no consigue sincronizarse, o bien no distingue la señalización correcta para sincronizarse, o se intenta sincronizar con una señal de control emitida por el inhibidor, en cualquier caso se bloquea la sincronización. Esto hace que nuestro sistema de inhibición sea más eficiente que los sistemas típicos que atacan con ruido gaussiano emitido a mucha potencia.

Previamente a la descripción en profundidad del funcionamiento del inhibidor, se describe el funcionamiento de la red GSM y su arquitectura, introduciendo también el uso de las tecnologías que le preceden y continúan.

Palabras clave
SDR; SCH; FCCH interferente; inhibidor; multi – trama; GSM

DEDICATORIA

Deseo expresar mi agradecimiento a todos aquellos que han hecho posible que haya llegado hasta aquí, por hacerme mejor persona y mejor ingeniero. En especial a mis padres a los que les dedico esta obra. Expreso también mi agradecimiento a todos los profesores que me han enseñado lo necesario para llegar hasta aquí, en especial a mi mentor en este proyecto, Víctor Pedro Gil Jiménez.

ÍNDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

1. INTRODUCCIÓN

1.1 Motivación.

Hoy en día las telecomunicaciones forman parte de nosotros, de tal forma que gente que ha nacido sin la existencia de internet o el teléfono ahora considera que no sería capaz de vivir sin todas las ventajas que nos proporcionan las telecomunicaciones.

Videojuegos, video-llamadas, redes sociales, somos muchas veces incapaces de separarnos de nuestros teléfonos móviles. Hay quien dice que estamos creando una dependencia exagerada de estas tecnologías pero lo cierto es que las telecomunicaciones nos ayudan a hacer cosas que nunca pensaríamos que podríamos hacer, estar más cerca de las personas más lejanas, encontrar pareja, entretenimiento, trabajo, defensa, salud, etc.

Por ello elegí esta carrera y por ello y por todo lo que demuestro a lo largo de este proyecto pienso en la necesidad de la existencia de los inhibidores de frecuencias, y cómo construir uno, iba a ayudarme a comprender mejor el uso de esta tecnología, con el único de fin de algún día poder mejorarla.

1.2 Objetivos.

El objetivo de este proyecto es crear un inhibidor de frecuencias en tecnología de radio definida por software(Software Defined Radio) para red de comunicaciones GSM (Global System for Mobile communications).

La tecnología de radio definida por software crea sistemas en los que elementos de comunicaciones típicamente implementados en hardware(moduladores, demoduladores, filtros, mezcladores) pasan a poder implementarse en software con la única necesidad de un ordenador o cualquier otro dispositivo de computación. Esta tecnología no es nueva, pero hace años era imposible de implementar de manera práctica ya que no se contaba con el poder de computación necesario para ello, actualmente disponemos en nuestro bolsillo de un poder de computación muy superior al que se tenía cuando se mandó el hombre a la luna y es probable que dentro de un tiempo la mayoría, si no toda la tecnología de comunicaciones, funcione con esta tecnología definida por software.

Se considera a Joseph Mitola III el desarrollador del concepto de equipos de radio-comunicación creados a partir de software. A partir de este concepto se han creado varias iniciativas públicas como la FLEX-500, la GNU radio o la HPSDR. Todo esto lleva a desembocar en lo que se conoce como radio cognitiva la cual puede hacer que emisor y receptor trabajen con la mejor opción en cada momento aprovechando al máximo el ancho de banda.

El hardware necesario para la implementación de un sistema SDR (Sofwtare Defined Radio) es muy sencillo, basta con un ordenador o sistema de computación con ADC (Analogic to Digital Converter), DAC (Digital to Analogic Converter) y una antena.

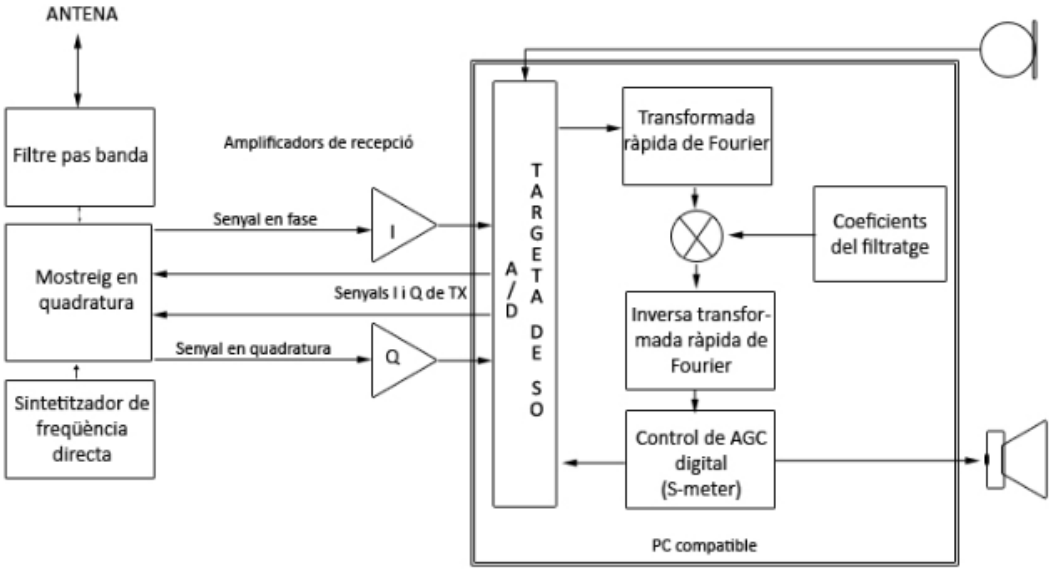

Figura 1.1 Implementación hardware de tecnología SDR con un ordenador, (figura tomada de: Wikipedia)

La tecnología SDR tiene un gran número de ventajas con respecto a la tecnología hardware que se utiliza actualmente. Permite emitir y recibir múltiples canales al mismo tiempo, es decir, es capaz de identificar el flujo de datos con el que está manteniendo la comunicación y además realizar varias tareas a la vez, además generalmente es interoperable con otros tipos de radio y soporta múltiples usuarios en la misma banda. Otra de las características que hacen la tecnología SDR muy apetecible es el hecho de que en caso de avería o simplemente en caso de necesidad de la actualización de la red, basta con actualizar el sistema en vez de reemplazar el dispositivo hardware al que esta tecnología sustituye, minimizando enormemente los costes de las telecomunicaciones.

En conclusión, la tecnología SDR proporciona un entorno más eficiente, modificable y flexible, puesto que modificando o sustituyendo sus programas de software, o añadiendo otros nuevos, se consigue cambiar sus funcionalidades. Este hecho permite especializar la SDR para cada usuario dependiendo de sus necesidades.

Todas estas cualidades hacen perfecta la tecnología SDR para la implementación de un inhibidor de frecuencias. En este caso voy a desarrollar un inhibidor de frecuencias para la red GSM, pero esta tecnología es perfectamente capaz de desarrollar inhibidores de frecuencias en el resto de redes conocidas.

2. PLANTEAMIENTO DEL PROBLEMA Y ESTADO DEL ARTE

2.1 Situación actual.

Entendemos por un inhibidor de frecuencias un dispositivo capaz de dificultar o impedir las comunicaciones por radiofrecuencia en un determinado espectro entre otros dispositivos que están dentro de su campo de alcance, pero, ¿Exactamente cómo funciona este objeto?

Un inhibidor de frecuencias consta de un generador de onda y un transmisor, cuyo objetivo no es eliminar ni suprimir determinadas frecuencias del espectro, si no producir un ruido suficientemente fuerte que imposibilite que el emisor y el receptor puedan establecer una comunicación. Para ello, el generador de onda a través de un oscilador, genera una señal sin información útil (ruido) que emite el transmisor a una potencia mayor que el sistema a interferir, logrando así volver completamente inútil la información transmitida por el sistema a interferir.

La necesidad de existencia de estos aparatos se debe al amplio uso que se le está dando progresivamente al espectro radioeléctrico y a las comunicaciones. Como era de esperar hay personas que son capaces de darle a estas tecnologías de comunicaciones un uso negativo o terrorista. Un ejemplo claro son las bombas por control remoto, ni siquiera es necesario estar en un lugar para hacer estallar una bomba, basta con enviar una señal de radio a ésta para ordenarla que explote. O por ejemplo evitar que salgan o entren de un lugar concreto comunicaciones, para mantener algún lugar secreto a salvo de cualquier señal. El caso es que existen usos muy peligrosos que se le pueden dar a las tecnologías de telecomunicaciones actualmente y por ello a veces simplemente conviene interferir estas señales.

Otra necesidad típicamente militar para la existencia de los inhibidores de frecuencia es su capacidad para evitar las comunicaciones del enemigo, uno de los objetivos históricos clave para la victoria consiste en dejar incomunicado a los soldados de sus generales y dirigentes. Pero esto no afecta únicamente a la guerra sobre el terreno, sin ir más lejos que un simple y sencillo micrófono que haya en nuestra casa o cualquier habitación es capaz de vulnerar nuestra libertad. Un ejemplo llamativo es el micrófono ruso que se consiguió introducir en la embajada Americana en Rusia durante la Guerra Fría. Éste aparato emitía ondas de radio para transmitir lo que se decía en la habitación y no fue detectado debido a que era pasivo, es decir, no necesitaba una fuente de alimentación externa. Este micrófono estuvo operativo cerca de 5 años. De la misma manera en las cárceles es necesario el uso de inhibidores para evitar comunicaciones tanto de entrada como de salida con el fin de evitar posibles fugas o el hecho de que el líder de una banda pueda seguir dando órdenes desde la cárcel.

Como toda nueva tecnología, esta no está absenta de que la usen inapropiadamente, por ejemplo, un inhibidor de frecuencias se puede utilizar para impedir las comunicaciones entre las autoridades o personas privadas, así como para burlar sistemas de seguridad

que se sirvan del espectro radioeléctrico para comunicar un fallo o una avería o simplemente una señal de video.

Este tipo de situaciones se habría evitado con un simple inhibidor, que aunque hubiese más de un micrófono escuchando no se podría transmitir la información. Por ello los inhibidores son una tecnología que estaba condenada a ser creada por necesidad, por culpa del aumento tecnológico que están sufriendo las radiocomunicaciones.

Estos casos también son razón de por qué el uso de los inhibidores de frecuencias queda enteramente reservado a las fuerzas de seguridad del estado y al ejército para dar protección a instituciones, coches y organismos oficiales y demás sitios que puedan ser objetivo de un atentado terrorista.

El problema queda planteado, tenemos una tecnología de radiocomunicaciones muy avanzada, que se puede utilizar inapropiadamente y prácticamente imparable, por lo que necesitamos alguna forma de limitarla o hacerla menos dañina. Al igual que el chaleco anti – balas se creó después que las pistolas, la necesidad de protegerse de estas armas de fuego es similar a la necesidad que hay ahora de defenderse de las radio – armas.

2.2 Diseños y comparación.

Actualmente podemos encontrar una diversa cantidad de dispositivos inhibidores entre los cuales podemos encontrar:

Inhibidores GPS, de radares, de telefonía, de dispositivos infrarrojo, de video, de audio, de drones… etc.

Obviamente una cosa es que existan varios tipos de inhibidores y otra cómo se inhibe la señal. En este proyecto vamos a implementar un sistema de inhibición que destaca por su eficiencia con respecto a otros sistemas típicos que funcionan mediante fuerza bruta.

Por ejemplo, los inhibidores convencionales transmiten ruido en la banda de frecuencias de la red que se desea inhibir, como utiliza el sistema descrito en la patente ES3311305 B1, la cual describe el funcionamiento para la inhibición de la red GSM, pero que debido al espectro ensanchado de las redes de generaciones superiores, no funciona en ellas.

En el funcionamiento del inhibidor de esta patente se utiliza un procedimiento dinámico de control y conmutación de antenas. Un dispositivo mediante una serie de operaciones de control, recibe y evalúa los parámetros (velocidad, posición, etc.) del entorno del vehículo protegido por el inhibidor y que pueden afectar a la cobertura de la señal de inhibición. En función de estos parámetros existe un algoritmo de optimización mediante el cual el dispositivo de control selecciona la antena operativa, o bien la omnidireccional o la unidireccional frontal instalada en el vehículo [3].

Existen diversas patentes sobre formas eficientes de inhibición, como por ejemplo la patente US6456822B1 "Electronic device and method for blocking cellular communication" [1].

Esta patente describe un método y dispositivo capaz de inhibir de manera fiable llamadas telefónicas dentro de un área determinada. El dispositivo bloquea las frecuencias de control del sistema celular emitiendo una señal de bloqueo con una salida baja de potencia, que interfiere con la capacidad de recepción y de codificación de señales transmitidas por la estación base. Así se evita la rutina de aceptación de la conexión por parte del terminal móvil a la red. En esta patente se describe un funcionamiento tanto automático como remoto.

Este sistema es muy parecido al nuestro ya que ataca a los canales de control.

La siguiente es una patente china que describe el funcionamiento de un inhibidor multi – frecuencias: CN2424581Y "Omnibearing seeking multi-frequency wave inhibitor" [2].

En esta patente se describe un dispositivo de onda multi – frecuencia. Está compuesto por una parte de detección y control compuesta por una antena Y1, un filtro de paso de banda para cuero, un amplificador de bajo ruido y control de ganancia automático, un aislador, un circuito de detección de onda, un amplificador de CC, un tubo VOMS on-off y un empuje circuito de un relevo y otra parte de emisión compuesta por un generador de ondas, un modulo VCO, un circuito de amplificación de potencia, otro circuito de aislamiento y una antena. Cuando la antena de detección recibe las señales de comunicación de un teléfono, las ondas se filtran y la amplificación rectificadora empuja el relé para cerrarlo, por lo tanto la parte de emisión puede emitir en consecuencia y controlar la interferencia de la comunicación del teléfono durante largos periodos de tiempo. Éste dispositivo es adecuando para posiciones militares importantes o demás áreas sensibles o confidenciales.

Nuestra solución para la inhibición queda recogida en la patente ES2455067 A1 (14.04.2014) "Método y dispositivo para la inhibición de señales de telefonía movil" [3].

En ella se recoge el mecanismo de funcionamiento: "Método y dispositivo inhibidor de terminales móviles 3G y 4G que transmite una señal interferente en un canal de sincronismo primario, o en un canal de sincronismo secundario, o bien en el canal de sincronismo completo que comprende canales primario y secundario. La señal interferente puede ser la señal de sincronismo original que va en el canal de sincronismo a ser interferido pero desplazada en un número de muestras y/o de ranuras temporales. La interferencia del canal de sincronismo y, por tanto, inhibición de las señales de telefonía móvil puede generarse sin sincronización del inhibidor a la estación base que puede dar cobertura al terminal móvil interferido. Opcional y adicionalmente, se puede sincronizar con dicha estación base, obteniendo información del canal de sincronismo usado por la estación base, que se puede emplear en la generación de la señal de interferencia. Esta señal interferente requiere menos potencia que los inhibidores tradicionales." [3].

Aunque el dispositivo esté patentado referido a los terminales móviles 3G y 4G debido a que la tecnología UMTS (Universal Mobile Telecommunications System) y LTE

(Long Term Evolution) son de espectro ensanchado y además utiliza un acceso al medio por CDMA (Code Division Multiple Access), por lo tanto es necesaria mucha potencia para poder inhibir, por ello este sistema de inhibición se centró en estas tecnologías. Lo que es obvio es que en la red GSM la cual se puede inhibir por fuerza bruta, es decir, emitiendo ruido a mayor potencia con la que el terminal móvil recibe a la estación base gracias a que es una tecnología de espectro estrecho, se puede mejorar la inhibición en cuanto a eficiencia se refiere aplicando los conceptos en la presente patente.

Las patentes anteriores describen un funcionamiento similar al de fuerza bruta, el inhibidor para vehículos es en cuanto más sofisticado en términos de inhibición en movimiento ya que tienen que conseguir inhibir las señales emitidas hacia un vehículo en movimiento para lo cual necesita sensores de movimiento, clima y posición. Pero en general el uso de los inhibidores está arraigado a la fuerza bruta y de momento hay pocas patentes referidas al ataque de los canales de control, un método que describiremos en profundidad en los próximos capítulos.

3. HISTORIA DE LAS COMUNICACIONES

3.1 Introducción.

Para entender el funcionamiento de este proyecto, antes voy a explicar cómo y de donde nacen las tecnologías de telecomunicaciones hasta llegar a la red GSM e introduciendo brevemente las tecnologías que la continúan.

3.2 Inicios de la telefonía móvil.

La comunicación por radio apareció como alternativa a la comunicación por cable debido a sus obvias limitaciones espaciales.

El primer servicio de telefonía móvil comercial apareció en Estados Unidos en 1946 donde la compañía AT&T (American Telephone and Telegraph) comenzó a operar con MTSs (Mobile Telephone System) aunque debido a las limitaciones del espectro de radiofrecuencia, este sistema solo contaba con un máximo de 6 canales.

Estos sistemas aún no eran celulares y cada móvil contaba con un transmisor que abarcaba con una frecuencia fija toda la ciudad, empleando una gran potencia y desaprovechando el espectro de radiofrecuencia. Básicamente cada móvil era como una estación de radio para toda la ciudad y este sistema podía contar como mucho con unos 50 canales.

3.3 Tecnología celular.

La tecnología celular consiste en dividir el espacio en pequeñas áreas denominadas celdas de manera de que en vez de que haya una antena central a la que se conectan todos los sistemas, haya diferentes celdas en el espacio, cada una con una antena a la que se pueden conectar los sistemas. Este método es mucho más eficiente ya que permite reutilizar las frecuencias en cada celda de manera que cuanto más pequeña es la celda más frecuencias se pueden reutilizar y esto se traduce a un uso muy eficiente del espectro de radiofrecuencia y por lo tanto la posibilidad de conectar más usuarios.

La tecnología celular ya existía en 1947 en los Laboratorios Bell, pero para que funcionase esta tecnología se requería de una capacidad de computación de la que no se disponía en aquel momento, ya que, para que la red celular tuviese éxito necesitaría que un usuario pudiese cambiar de celda sin necesidad de que se cortase la llamada y esto requería de un sistema capaz de saber qué usuario se está moviendo y hacia dónde se está moviendo.

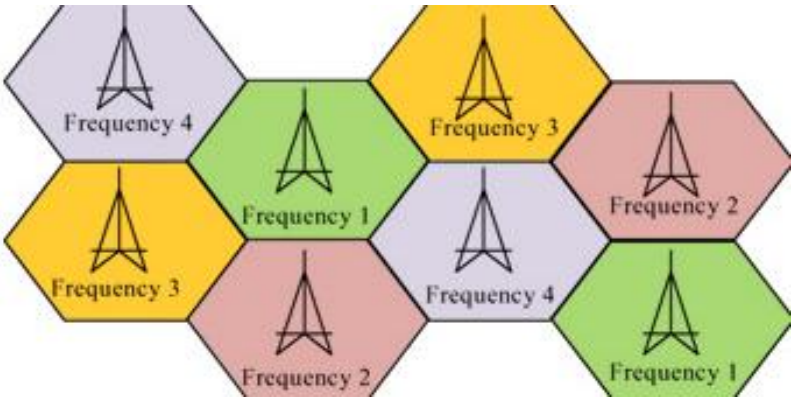

Figura 3.1, Reutilización de frecuencias en una red de celdas, (figura tomada de: http://www.wikiwand.com/es/Historia_del_tel%C3%A9fono_m%C3%B3vil)

El único requisito de una red celular es encontrar una manera de que cada celda distinga la señal de su propio transmisor de la señal de otros transmisores. Para ello hay 3 soluciones de acceso al medio: FDMA (Frequency Division Multiple Access), TDMA (Time Division Multiple Access), CDMA (Code Division Multiple Access) y SDMA (Space Division Multiple Access).

En SDMA se puede considerar como la más sencilla, consiste en segmentar el espacio en sectores utilizando antenas unidireccionales.

En FDMA el acceso al medio se realiza dividiendo el espectro de radiofrecuencia en canales que corresponden a distintos rangos de frecuencia, de manera que a cada usuario le corresponderá un canal. Los canales están separados por una banda de paso para no interferirse entre ellos. Esta es una técnica de multiplexación que se puede emplear tanto en protocolos digitales como analógicos.

En TDMA lo que se divide es un canal en pequeñas porciones de tiempo, también conocidos como slots. Gracias a estos slots se puede utilizar el mismo canal para varios usuarios proporcionando acceso múltiple a un reducido número de frecuencias. Un ejemplo sencillo para entenderlo mejor, si tenemos un canal y dos usuarios y queremos hacer TDMA, vale con asignar diferentes tiempos a cada usuario, por ejemplo el tiempo en segundos pares corresponde a un usuario y los segundos impares al otro, además en el receptor de cada usuario se ignoran los tiempos del otro por lo que cada usuario solo lee su información. Se utiliza sólo en comunicaciones digitales y aprovecha todo el ancho de banda.

A diferencia de los anteriores, CDMA utiliza el mismo canal a la misma frecuencia y al mismo tiempo para varios usuarios pero en este caso el acceso al medio se hace a través de códigos ortogonales, es decir, utiliza una codificación especial para cada usuario escogido de manera que sea ortogonal a los demás códigos. Esto provoca que no haya interferencias entre los usuarios porque lo que ve uno con respecto al otro es nulo.

Una analogía para entender la diferencia de estos tres métodos de acceso al medio podría ser una situación en la que tenemos a varias personas hablando a la vez en una

habitación. FDMA consistiría en que para no interferirse cada grupo de personas habla en diferentes frecuencias, más agudo o más grave. En TDMA para no interferirse lo que habría que hacer es que cada grupo de personas habla en diferentes tiempos y por último en CDMA la analogía seria que cada grupo de personas hablase en un idioma de manera que un grupo de personas solo puede entender el idioma en el que habla su grupo.

Este paso fue muy importante en la historia de las comunicaciones porque en el momento en el que se tiene capacidad para suficientes usuarios deseosos de estar conectados, se crea una relación oferta-demanda que tendrán un gran potencial económico y llevará a muchas empresas a desarrollar nuevas redes de comunicaciones para satisfacer esta necesidad.

En la siguiente figura mostramos el aumento del número de líneas telefónicas móviles y la penetración en Europa hasta 2017 y las previsiones para 2025.

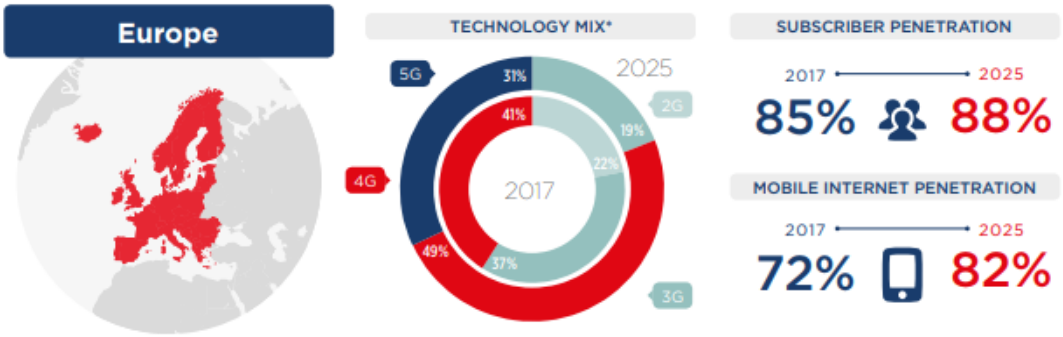

Figura 3.2, Aumento de las líneas móviles en Europa y penetración, (figura tomada de: https://www.gsma.com/mobileeconomy/wp-content/uploads/2018/05/The-Mobile-Economy-2018.pdf).

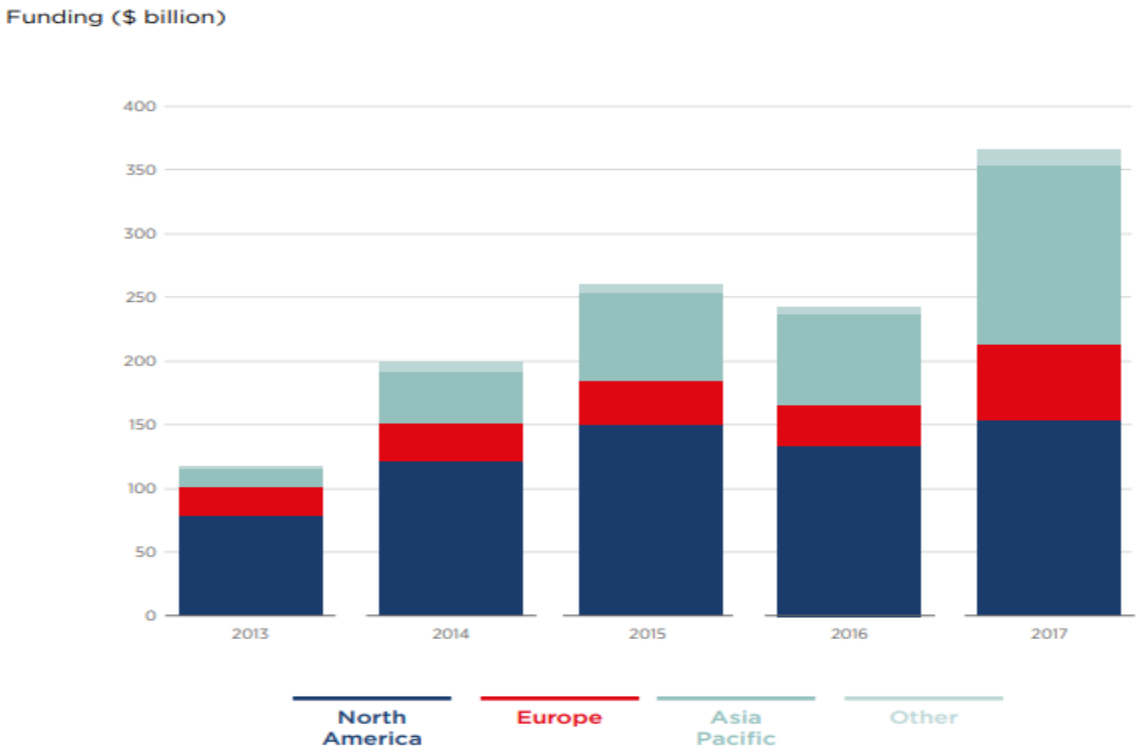

Figura 3.3, Inversión en las telecomunicaciones por parte del sector privado (figura tomada de: https://www.gsma.com/mobileeconomy/wp-content/uploads/2018/05/The-Mobile-Economy-2018.pdf).

Para hacernos una idea del impacto de la evolución de las comunicaciones, en 2017 las tecnologías y servicios de telefonía móvil generaron el 4.5% del PIB del mundo, con un valor de 3.6 billones de dólares. Además se han generado alrededor de 29 millones de puestos de trabajo directa o indirectamente por todo el mundo y han enriquecido al sector público en 500 mil millones de dólares en impuestos y a través de subastas del espectro radioeléctrico.

3.4 Primera generación.

El estándar AMPS (Advanced Mobile Phone System) fue el primero en abrirse camino junto con TACS (Total Access Comunication System), lanzado por NTT (Nippon Denshin Denwa Kabushiki-gaisha) en Japón en 1979 con el primer teléfono personal de la marca Motorola seguida por el lanzamiento del sistema NMT (Telefonía Móvil Nórdica) en Dinamarca, Finlandia, Noruega y Suecia, en 1981 mediante la marca Ericcson.

Esta primera generación contaba con servicio sólo de voz en tecnología analógica, multiplexación FDMA, alcanzaba una velocidad de entre 1 Kbps y 2.4 Kbps mediante conmutación de circuitos y funcionaba en la banda 800-900 MHz. Contaba con un ancho de banda de 30 KHz con capacidad para unos 832 canales de los cuales 21 estaban reservados para la conexión de la llamada.

3.5 Segunda generación, GSM.

En la década de 1990 nace GSM (Global System for Mobile communications), en la conferencia de telecomunicaciones CEPT (Committee of European Postal & Telephone). Se trata de un estándar europeo que contaba con la gran ventaja de las comunicaciones digitales.

La diferencia de las comunicaciones digitales con las analógicas reside en que las comunicaciones digitales prestan mayor calidad de servicio tanto en la calidad de la llamada como en la seguridad de la información ya que los datos de la llamada son codificados, además de que la tecnología digital posibilita que el tamaño del terminal sea mucho más reducido proporcionando un teléfono móvil más pequeño y manejable.

GSM cuenta con canales de 200 kHz. Cada canal tiene una capacidad de 270.833 kbps y para datos un máximo de 9.6 kbps en un canal, esta es una de las principales razones por las que se pasa a la tercera generación ya que las aplicaciones multimedia comenzaban a necesitar de mayor velocidad. Máxima potencia de transmisión del terminal de 2W que desciende a 1W en la banda GSM 1800MHz, 1900MHz.

GSM apareció en Europa en la banda 900 MHz y 1800 MHz, en cambio en Estados Unidos en la banda 1900 MHz, la razón de esto fue meramente por motivos legales y por la disponibilidad de frecuencias no asignadas.

Aquí tenemos una tabla que muestra las frecuencias utilizadas por la red GSM tanto por el DL (Down Link) como por el UL (Up Link) y los canales que utilizan.

BANDAS DE FRECUENCIA PARA GSM

Banda	Nombre	Canales	Uplink (MHz)	Downlink (MHz)	Notas
GSM 850	GSM 850	128 - 251	824,0 - 849,0	869,0 - 894,0	Usada en los EE.UU., Sudamérica y Asia.
GSM 900	P-GSM 900	1-124	890,0 - 915,0	935,0 - 960,0	La banda con que nació GSM en Europa y la más extendida
	E-GSM 900	975 - 1023	880,0 - 890,0	925,0 - 935,0	E-GSM, extensión de GSM 900
GSM1800	GSM 1800	512 - 885	1710,0 - 1785,0	1805,0 - 1880,0	Europa y muchos otros países
GSM1900	GSM 1900	512 - 810	1850,0 - 1910,0	1930,0 - 1990,0	Usada en Norteamérica, incompatible con GSM-1800 por solapamiento de bandas.

Tabla 3.1, bandas de frecuencia para GSM, (tabla tomada de: http://ocw.uc3m.es/ingenieria-telematica/aplicaciones-moviles/material-de-clase-2/inalambricos)

La modulación utilizada en GSM es la GMSK (Gaussian Minimum Shift Keying) cuya constelación aparece en la siguiente figura, mostramos la constelación porque se observa de manera grafica y sencilla la evolución con respecto las próximas generaciones. En GMSK se envía un bit por símbolo, generando la siguiente constelación.

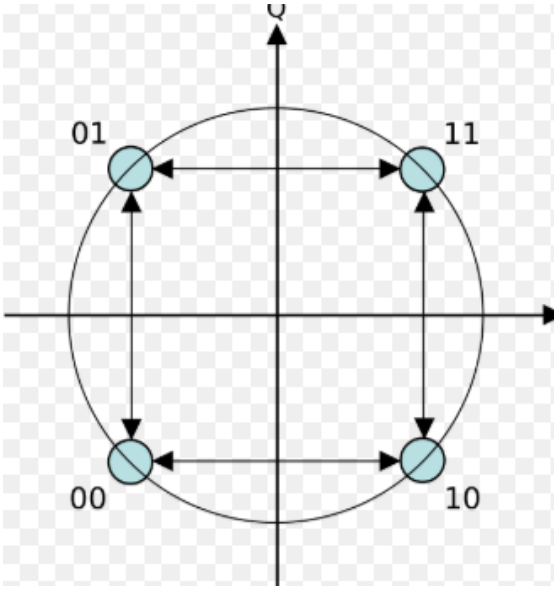

Figura 3.4, Constelación GMSK, (figura tomada de: Wikipedia)

GSM funciona por conmutación de circuitos y el acceso al medio lo hace con TDMA aunque también se puede utilizar FDMA complementándose con un cambio de canal

según las necesidades de la red denominado frequency hopping. También se puede utilizar CDMA pero esta vez se aumenta el ancho del canal a 1.23 MHz.

Entre los servicios ofrecidos está:

• Voz digital.
• SMS.
• Roaming internacional.
• Llamada en espera, bloqueo de llamada y retención de llamada.

Por todo ello se considera la red GSM la primera red móvil digital funcional.

3.6 Generación 2.5.

La generación 2.5 existe porque se mejoraba a la red GSM en términos de velocidad y servicio, pero no lo suficiente como exigía la tercera generación.

Pasamos de la conmutación de circuitos a la conmutación de paquetes lo cual aumenta la eficiencia de uso de canal ya que en conmutación de circuitos si se transmite en un porcentaje pequeño se está desaprovechando el canal.

Los estándares de esta generación son: GPRS (General Paquet Radio Service), HSCSD (High-Speed Circuit-Switched Data) y EDGE (Enhaced Data rates for GSM Evolution), este último es considerado como la generación 2.75, todo ellos basados en GSM.

GPRS contaba con una velocidad de entre 56Kbps y 114 Kbps, HSCSD hasta 38.4 Kbps y EDGE hasta los 384 Kbps funcionando en la banda de 2100 Hz

En cuanto a la modulación GPRS y HSCSD utilizan GMSK mientras que EDGE utiliza una 8-PSK la cual utiliza 3 bits por símbolo, generando la siguiente constelación.

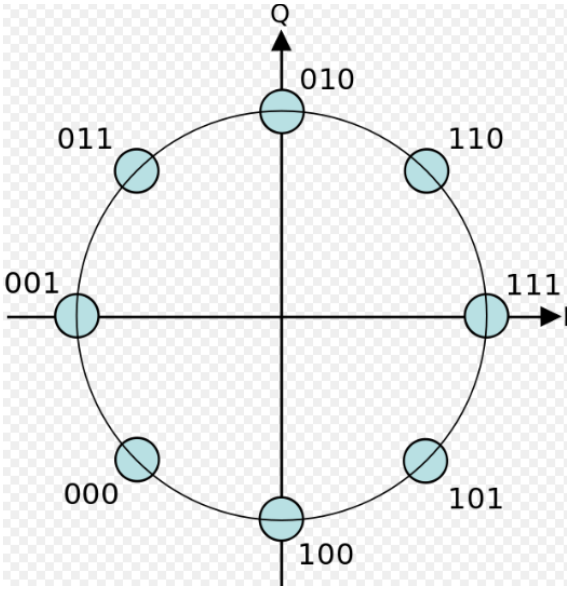

Figura 3.5, Constelación 8 – PSK, (figura tomada de: Wikipedia)

Entre los nuevos servicios ofrecidos se encuentran los siguientes:

• Servicios multimedia.
• Videoconferencia.
• Búsqueda y directorio.
• Juegos móviles.

3.7 Tercera generación, UMTS.

El objetivo de la tercera generación consiste en aumentar la capacidad de transmisión de datos para tener mayor capacidad de voz y datos con el fin de soportar aplicaciones como la televisión, internet desde el móvil y descarga de archivos, todo ello a un bajo coste. En esta generación la voz se conmuta mediante circuitos y los datos mediante paquetes.

En cuanto al estándar utilizado, es por excelencia UMTS (Universal Mobile Telecommunications System) en Europa y Japón basado en tecnología W – CDMA (Wideband Code División Multiple Access), pero incialmente la ITU (International Telecommunication Union) definio la red 3G con el estándar IMT-2000, trabajo continuado por la organización 3GPP (3rd Generation Partnership Project). En América se utiliza EV – DO (Evolution – Data Optimized) estandarizado por 3GPP2.

UMTS puede alcanzar una tasa de transferencia de datos desde 144 Kbps hasta 512 Kbps en superficies de cobertura amplias, en áreas locales puede llegar a los 2 Mbps. Tiene un ancho de banda de 5 MHz a 20 MHz.

A lo largo de la tercera generación UMTS se ha actualizado, primero se incluyó HSDPA que optimiza la tecnología espectral llegando a alcanzar los 14 MBps. Después se introdujo HSUPA que aumentaba la tasa de subida de datos a 7.2 Mbps, aunque la máxima modificación a la que llegara UMTS es con HSPA logrando velocidades de 56 Mbps de bajada y 22 Mbps de subida de datos utilizando tecnología MIMO.

La modulación utilizada por UMTS es la modulación QAM la cual asigna 4 bits a cada símbolo, en el caso de una 16 QAM se genera la siguiente constelación, pero UMTS en su máxima actualización alcanza a utilizar una 64 QAM.

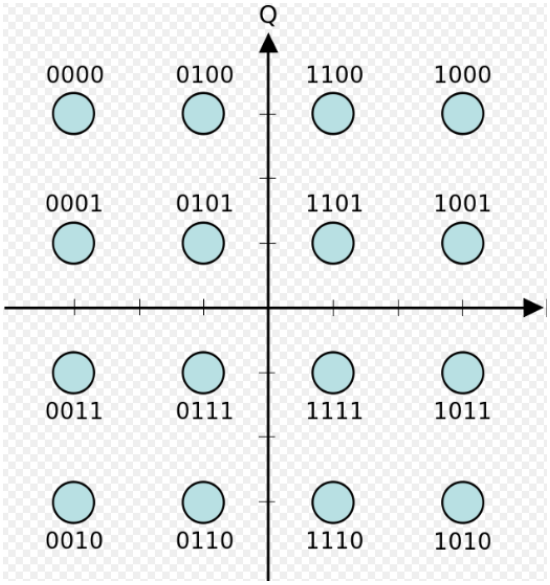

Figura 3.6, Constelación 16 QAM, (Figura tomada de: Wikipedia)

Entre los nuevos servicios ofrecidos por UMTS se encuentran los siguientes:

• Acceso a internet de alta velocidad.
• Llamadas de video, chat y conferencia.
• Televisión móvil.
• Servicios de geolocalización.
• Correo electrónico.
• Busca-personas.
• Banca virtual y servicios climatológicos.

3.8 Cuarta generación, LTE.

El sistema de la cuarta generación está basado completamente en tecnología sobre IP, el objetivo principal de esta tecnología es proporcionar más velocidad, más calidad y más capacidad, aparte de dar mayor seguridad.

El estándar utilizado por esta generación es LTE (Long Term Evolution) estandarizado por 3GPP (3rd Generation Partnership Project), aunque también existe WiMAX móvil estandarizado por el IEEE (Institute of Electrical and Electronics Engineers).

La velocidad que se alcanza en esta generación va desde los 100 Mbps a 1Gbps con toda la red disponible. El acceso al medio se realiza generalmente con OFDMA para el enlace descendente, que es un método de acceso múltiple basado en FDMA con las portadoras ortogonales de forma que se pueden utilizar más portadoras con un menor ancho de banda, CDMA y variantes como MC – CDMA y LAS – Red – LMDS. El ancho de banda es más amplio llegando a 40 MHz.

La modulación que se utiliza en LTE es una 64 QAM que es igual que la representada anteriormente solo que con 64 elementos en vez de 16, esto significa que se utilizan 6 bits por símbolo en vez de 4.

Las bandas de frecuencia utilizadas por LTE son de 2500 MHz en América y los 2600 MHz en Europa.

Entre los nuevos servicios ofrecidos por LTE se encuentran los siguientes:

• Telefonía IP.
• Televisión 3D.
• Televisión móvil de alta definición.
• Computación en la nube.
• Digital Video Broadcasting (DVB).
• Dispositivos portátiles.

3.9 Quinta generación.

Aunque aún no esté implementada vamos a introducir la tecnología de la quinta generación.

La quinta generación es considerada una tecnología OWA (Open Wireless Architecture). Para realizar esto la capa de red está subdividida en dos capas, la de red superior para el terminal móvil y la de nivel inferior para la interfaz de red. Todo el enrutamiento en la quinta generación se basa en direcciones IP.

El objetivo es el mismo de siempre, mayor velocidad, seguridad y calidad, es decir, un poco más de todo. Esta tecnología utiliza el OTP (Open Transport Protocol) soportado por la capa de transporte, es la encargada de superar la pérdida de velocidad de bits en IP.

En la quinta generación la velocidad se aumenta de 1 Gbps a 10 Gbps, el ancho de banda se mide por unidad de superficie, funciona en la banda de 3 GHz a 300 GHz. El acceso al medio se realiza mediante CDMA y BDMA. Los estándares que se utilizan en 5G son los que se utilizan en IP; IP – LAN, WAN, PAN y WWWW.

Ente otras características que trae la quinta generación está: muy alta velocidad, reducir prácticamente al nulo la latencia y el retardo, infraestructura virtualizada y la reducción del 90% del consumo de energía en la red.

La cantidad de nuevos servicios que puede ofrecer la red 5G es sumamente grande ya que convertiría el mundo en una zona WiFi.

4. DESCRIPCIÓN DEL PROYECTO

4.1 Profundización en GSM

En el apartado anterior he presentado la red GSM, ahora voy a profundizar en ella para mostrar cómo funciona y cómo vamos a inhibirla.

La red GSM funciona con tecnología celular, está formada por varias estaciones base que, cada una de ellas consta de una antena con un radio de cobertura siendo este radio el tamaño de la celda. Una estación base puede alcanzar diferentes radios de cobertura debido a que en este caso el radio necesario en zonas rurales es diferente al de las ciudades, claro está porque la cantidad de usuarios depende del ancho de banda y en las ciudades se necesitarán más estaciones base de pocos cientos de metros de radio porque las ciudades tienen muchos usuarios en poco espacio, mientras que las zonas rurales tienen pocos usuarios en mucho espacio y aquí las estaciones base pueden alcanzar un radio de 35 Km.

La red GSM utiliza para mayor eficiencia TDMA, así el terminal no está transmitiendo todo el transcurso de la llamada y se ahorra batería. En GSM el tiempo se divide en slots de 576.9 μs, se reserva el primero de ellos para la sincronización, por parte de la estación base por el DL y otro slot para recibir, el resto de slots quedan libres para el uso de usuarios. Esto permite un buen aprovechamiento del espectro disponible y una duración mayor de la batería al transmitir el terminal solo las fracciones de tiempo que le pertenecen.

Las estaciones base están a su vez conectadas a un controlador de estaciones base (BSC) el cual administra los recursos que se les proporciona a las estaciones base en cuanto a reparto de frecuencias y control de la potencia con la que emite cada estación base.

El BSC también es el encargado de que no se corte la comunicación al cambiar de celda, esto se hace gracias a que las estaciones base miden la potencia con la que reciben a un terminal y envían esos datos a el BSC de manera que esta puede triangular donde se encuentra el terminal y deducir cómo se desplaza, por lo tanto cuando el BSC observa que un terminal va a pasar de una celda a otra avisa al centro de conmutación móvil (MSC) al cual está físicamente conectado y al terminal para hacer el salto. Este proceso se conoce como handover o handoff y también se puede dar en ocasiones en las que la estación base más cercana al terminal esté saturada y se conecte a la siguiente más cercana. El MSC pertenece al subsistema de conmutación de red (NSS) el cual gestiona las identidades de los usuarios, ubicación y establecimiento de comunicaciones con otros usuarios.

El MSC gestiona todo eso conectándose a bases de datos como el registro de ubicación de origen (HLR), una base de datos que contiene información en relación a la ubicación de los usuarios registrados dentro de la zona del MSC, cada red debe tener al menos un HLR. También se conecta al registro de ubicación de visitante (VLR), esta es una base de datos que contiene información de los usuarios que no son abonados locales a la MSC de esa región, ciertamente es un registro de invitados. El VLR recoge los datos de un visitante del HLR y los mantiene hasta que el visitante abandone la zona de MSC en la que se encuentra o después de un periodo de inactividad.

Otros registros a los que se conecta el MSC son el registro de identificación de equipo (EIR), el cual almacena los IMEI, un número de 15 dígitos que es utilizado por el EIR para generar listas blancas o negras con el fin de reducir las probabilidades de robo de terminales o fraude. También contiene la lista de terminales móviles y el centro de autenticación (AUC) que se encarga de verificar las identidades de los usuarios, está asociado al HLR y contiene las claves de identificación de los usuarios, una clave secreta de 128 bits (SIM) que no abandona el AUC y un conjunto de tres claves que se conoce como el triplete de autenticación. En la siguiente figura mostramos gráficamente la arquitectura de GSM.

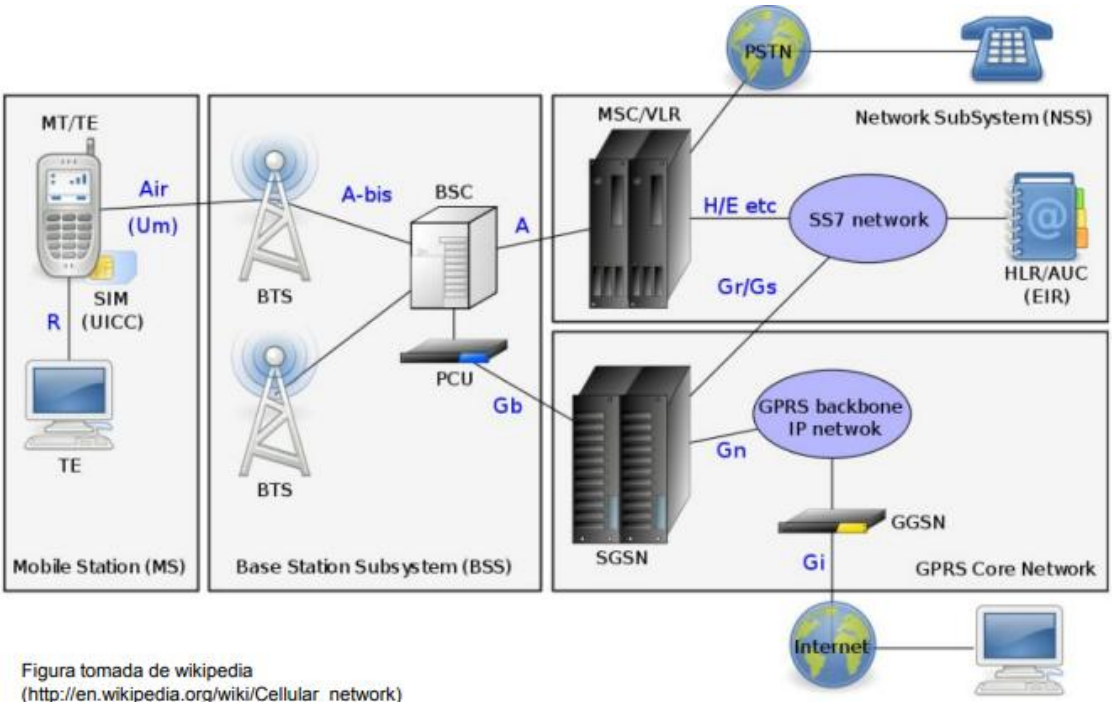

Figura 4.1, Arquitectura de la red GSM. (Figura tomada de: http://ocw.uc3m.es/ingenieria-telematica/aplicaciones-moviles/material-de-clase-2/inalambricos)

Algo nuevo que se introdujo en la red GSM es la tarjeta SIM la cual contiene información como el número de teléfono del abonado (MSISDN), el numero internacional del abonado (IMSI), el código de servicio, es decir el operador al que pertenece, la clave y autenticación (código PIN) y el código personal de desbloqueo (PUK), estos dos últimos son códigos personales. Todo esto proporcionó a GSM una gran seguridad en las comunicaciones.

En GSM también se introdujo el concepto del roaming que consiste en la capacidad de los dispositivos móviles de poder utilizar una red que no sea la suya principal, por ejemplo redes de otros operadores.

Ahora que ya conocemos la arquitectura, vamos a profundizar en cómo funciona GSM internamente, es decir, estudiar cómo establece la conexión de la llamada que es lo que nos interesa para saber cómo sabotearlo, inhibirlo.

La modulación que utiliza GSM es una GMSK, pero puesto que esta es una variante de la modulación MSK (Minimum-shift keying), explicaremos antes esta modulación.

La modulación MSK es una modulación por desplazamiento de frecuencia continua, codificado con bits alternantes entre los componentes de cuadratura donde el componente " a_Q" está retrasada por la mitad del periodo de símbolo codificado con cada bit como media sinusoide dando a lugar una señal envolvente constante la cual reduce los problemas de distorsión no lineal. En la MSK la diferencia entre la frecuencia inferior y superior es de exactamente la mitad de la tasa de bit, por lo que la desviación máxima de frecuencia es el 25% de la frecuencia máxima de modulación por lo tanto el índice de modulación es de 0.5 lo cual provoca que las ondas para representar un cero y un uno son ortogonales. A continuación la expresión matemática de la MSK.

$$s(t) = a_I(t)\cos\frac{\pi t}{2T}\cos 2\pi f_c t - a_Q(t)\sin\frac{\pi t}{2T}\sin 2\pi f_c t \qquad (4.1)$$

La modulación GMSK aunque es similar a la modulación MSK, la diferencia es que su flujo de datos atraviesa previamente un filtro paso bajo gaussiano antes de llegar al circuito modulador, generando un efecto suavizador que reduce el ancho de banda necesario y a su vez se reduce la interferencia que viene de las portadoras de frecuencias adyacentes que hay fuera de la banda de paso. El único problema que introduce el filtro es que el pulso a su salida es mayor que el tiempo de un bit por lo que esto puede generar que haya interferencia entre símbolos, pero con una ecualización adaptativa en el receptor se subsana este contratiempo.

Ya conocemos como funciona la arquitectura de GSM y la modulación que usa pero lo más importante para saber cómo inhibirlo es ver cómo se sincroniza el terminal móvil a la estación base. Para ello vamos a centrarnos en el enlace de bajada ya que es mediante el cual la estación base envía al terminal móvil los elementos de control para su sincronización.

GSM utiliza varios tipos de canales, canales de tráfico (TCH), de control entre los cuales existen los canales de difusión (FCCH, SCH, BCCH), comunes (CCCH, RACH, PCH, AGCH) y dedicados (SADCCH, SACCH, FACCH). Pero nosotros vamos a centrarnos en los canales de control de difusión ya que estos son mediante los cuales la estación base consigue sincronizar al terminal móvil, todos ellos van por el enlace descendente.

Cuando se enciende el terminal móvil, éste se sintoniza en frecuencia y en tiempo, después decodifica los canales BCCH y se comprueba si la SIM es válida en la red, se actualiza la localización y se autentica.

El canal FCCH se utiliza para la sincronización de la estación base con el terminal móvil, consiste en una ráfaga de ceros modulados con una GMSK que produce una señal sinusoidal continua que sirve para mostrar al terminal móvil a la frecuencia a la que tiene que sincronizarse.

El SCH, una vez sincronizado en frecuencia el terminal móvil a la estación base, se necesita el sincronizado en tiempo. El SCH lleva en él el número de la trama y el BSIC que es el código de identidad de la estación base, el cual indica a qué estación base se está conectando el terminal móvil. El canal SCH está compuesto de 25 bits de información divididos en 19 bits para el numero de cuadro reducido, 6 bits para el

BSIC, 3 bits de BCC el cual es el código de colores de la estación base y otros 3 bits de NCC que es el código de colores de la red.

El canal BCCH lo que hace es enviar información de señalización a todos los terminales de la celda segregados en pequeños mensajes llamados mensajes del sistema, para llevar toda la información completa se necesitan 4 BCCHs consecutivos en el primer intervalo de la multi – trama 51, aunque si es necesario también se pueden enviar en los siguientes intervalos.

Entre la información que contiene el BCCH está:

• Identidad de la red GSM.

• Frecuencias usadas en la celda y las celdas vecinas.

• Información en relación al VLR.

• Máxima potencia a usar en los canales de control.

• Número máximo de repeticiones de canal de control.

• Número de time slots para paging y asignación.

La estación base transmite continuamente mensajes del sistema los cuales ayuda a los terminales móviles a determinar si pueden o no conectarse a la celda, algunos de estos mensajes son obligatorios y otros opcionales y algunos se tienen que transmitir por el SACCH. Los diferentes mensajes del sistema que se pueden transmitir son los siguientes:

•SI-1: Los parámetros ARFCN y RACH necesarios para acceder al sistema y la información relacionada con el salto de celda se envían en este mensaje.

•SI-2: Las frecuencias vecinas BCCH y la información PLMN se envían en este mensaje. Estas frecuencias se usan para mediciones de intensidad de señal requeridas para el handover.

• SI-2bis: información sobre las celdas vecinas.

• SI-2ter: información de BCCH extendido asignado en qué células vecinas se proporcionan en este SI. Transmitido opcionalmente en BCCH por la red a todas los terminales móviles.

• SI-2quater: Información sobre las celdas 3G vecinas

• SI-3: LAI del área de ubicación actual, identidad de celda, información de canal de control requerida para calcular el grupo de buscapersonas, opciones de celda para lograr un buen rendimiento en la celda, parámetros de selección de celda requeridos por el terminal móvil.

• SI-4: La información de frecuencia relacionada con CBCH y CBCH, LAI, parámetros de selección de celda e información de control de RACH.

• SI-5: Transporta información de células vecinas. El terminal móvil envía informes de medición en el enlace ascendente y la información de potencia de salida en el enlace

descendente (en SACCH). También obtiene información relacionada con el proveedor BCCH de las celdas vecinas.

• SI-6: La información sobre LAI, opciones de celda, identidad de celda y PLMN permitido.

• SI-7: Parámetros de re-selección de celda.

• SI-8: Parámetros de re-selección de celda.

• SI-9: Información sobre la estructura de los mensajes del sistema.

• SI-13: Información sobre portadora de GPRS necesaria para una llamada PS.

A continuación mostramos en la siguiente figura las diferentes tramas que utilizan los canales de GSM a nivel más bajo.

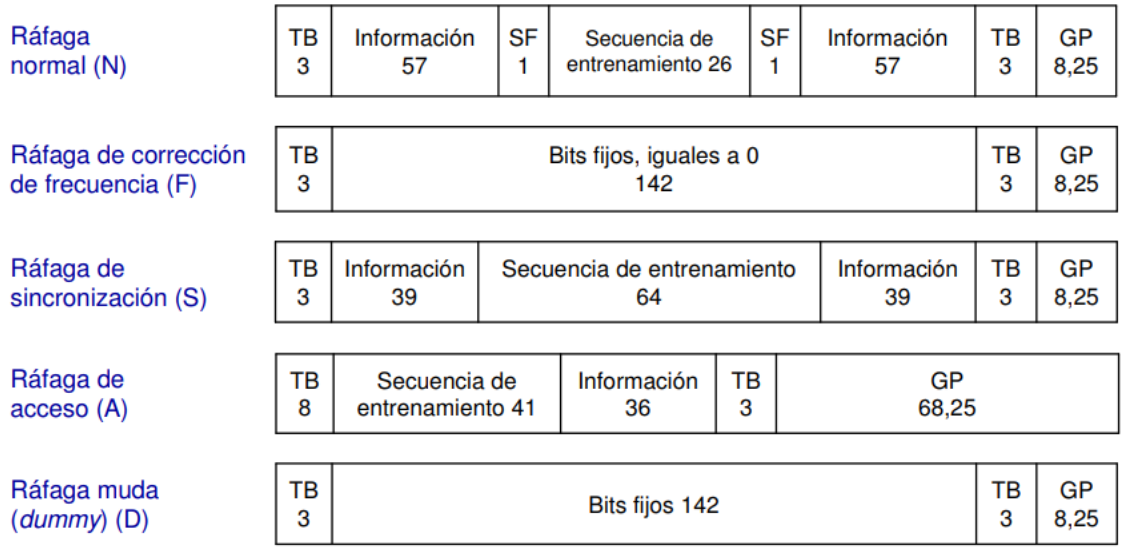

Figura 4.2, Diferentes tramas utilizadas por los canales de GSM. (Figura tomada de: http://ocw.upm.es/teoria-de-la-senal-y-comunicaciones-1/comunicaciones-moviles/contenidos/tema-6)

Donde TB significa bits de cola, se ponen al principio y al final de los datos, GP el periodo de guarda al final de cada trama para evitar solapamiento y SF un flag. Las siglas están en inglés.

De los canales que nos interesan el FCCH utiliza la ráfaga de corrección de frecuencia (F), el SCH utiliza la ráfaga de sincronización (S) y el BCCH utiliza la ráfaga normal (N). Aunque no vayamos a utilizarlo para la inhibición la ráfaga de acceso (A) la utiliza el canal RACH y por último la ráfaga muda se envía en casos en los que no hay información que transmitir. El resto de canales al igual que el BCCH utiliza la trama normal. Como se observa el tamaño de cualquiera de estas tramas es de 156.25 bits.

Todos estos canales van en la conocida como multi – trama 51. Es una multi – trama de 51 slots en el que cada slot contiene la trama del canal y en la que se observa claramente cómo se utiliza TDMA en GSM. Jerárquicamente hablando hay otra multi – trama de 27 tramas la cual se utiliza para tráfico y canales de control asociados y estas dos a su vez se recogen en súper – tramas e híper – tramas llegando a un total de 2047 tramas, pero

nosotros vamos a centrarnos en la multi – trama de 51 tramas ya que es la que contiene los canales de control de difusión que utilizaremos para inhibir.

A continuación en la figura, aparece representada la jerarquía de tramas en GSM incluyendo los tiempos que se tardaría en enviar cada una de ellas.

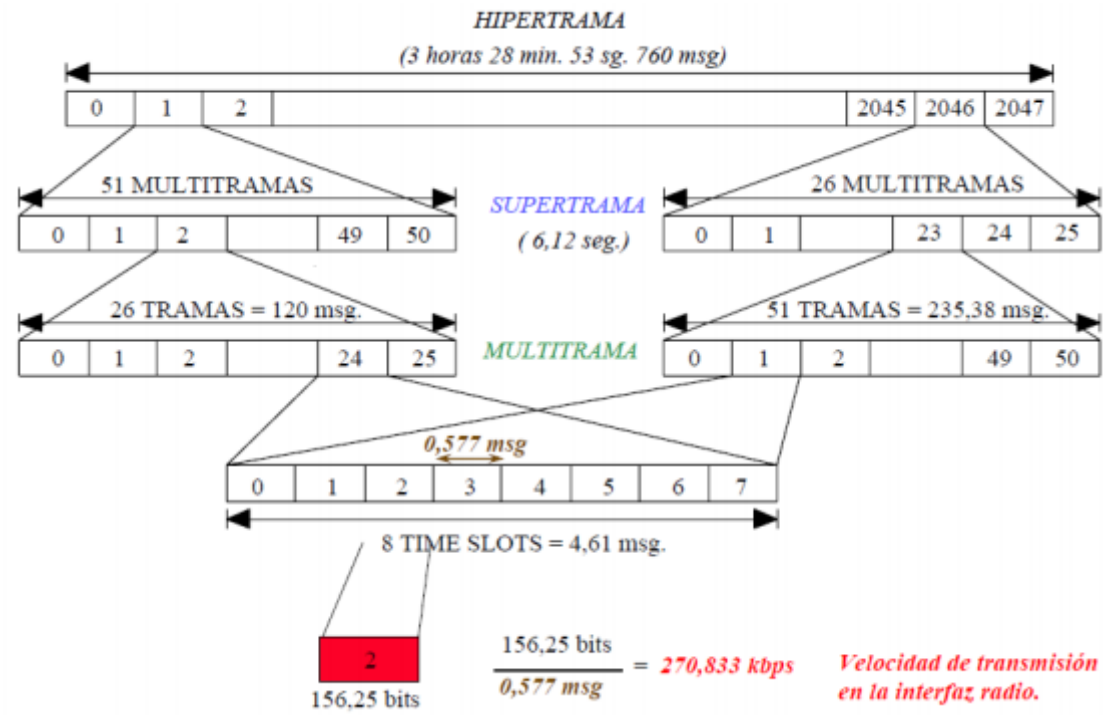

Figura 4.3, Estructura jerárquica de tramas en GSM. (Figura tomada de: http://bibing.us.es/proyectos/abreproy/70177/fichero/Carpeta+2%252FCapitulo2.pdf)

En la parte inferior de la imagen se calcula la velocidad de tasa de bit de GSM, el cálculo se debe a la cantidad de bits que hay en una trama al nivel más bajo, es decir las tramas representadas en la figura 4.2 dividido entre el tiempo que se tarda en enviar dicha trama, 0.577 ms.

Como hemos mencionado antes nosotros vamos a centrarnos en la multi – trama 51, por lo que vamos a hacer zoom en la anterior imagen y a sacar las características de esta multi – trama.

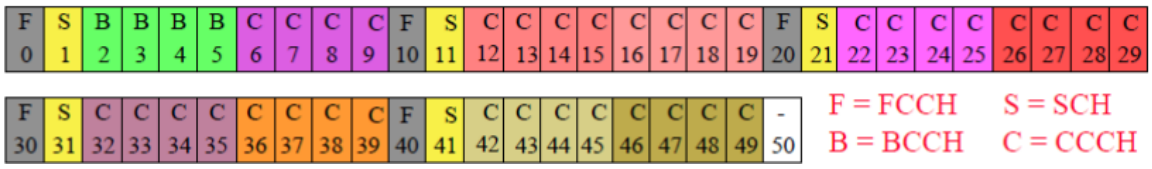

Figura 4.4, Multi – trama 51 (Figura tomada de: http://bibing.us.es/proyectos/abreproy/70177/fichero/Carpeta+2%252FCapitulo2.pdf)

Si observamos la trama vemos como el canal BCCH sólo se transmite en el primer intervalo, y que los canales FCCH y SCH se transmiten juntos y cada 10 slots. El canal CCCH se transmite en el resto de slots.

4.2 Solución escogida.

Pues muy bien, nuestro objetivo es evitar que el terminal móvil consiga distinguir correctamente los canales FCCH, BCCH o SCH ya que con que uno de estos canales no sea legible, el terminal móvil será incapaz de conectarse a la red GSM.

La idea principal de nuestra inhibición consiste en crear un canal FCCH falso al que hemos denominado FCCH interferente. Este FCCH interferente no contiene información útil, al contrario solo tiene ruido. El hecho de escoger este método consiste en que como el FCCH es una secuencia de ceros modulada con una GMSK hace muy sencillo su imitación y su transmisión en términos de potencia.

Una vez hemos creado nuestro FCCH interferente modulado con una GMSK, tenemos que enviarlo secuencialmente cada cierto tiempo, es decir, nosotros no conocemos el momento exacto en el que la estación base comienza a transmitir a nuestro terminal móvil para que se sincronice, entonces tenemos que pensar en una manera de que nuestros FCCH interferentes coincidan de alguna manera durante el tiempo en el que el terminal móvil se está intentado sincronizar. Para ello más a delante demostraré que lo más eficaz consiste en enviar nuestro FCCH interferente cada dos slots, de esta manera en algún momento siempre va a coincidir con más de un elemento de la multi – trama 51.

Cuando nuestro FCCH coincide con elementos de la multi – trama 51 hace de éstos ilegibles. La gran ventaja de inhibir con un FCCH interferente es que pueden ocurrir dos formas de inhibición, o bien el terminal móvil al encontrar nuestro FCCH interferente se sincronice a él obviamente con datos erróneos o bien recibe a la vez nuestro FCCH interferente con otros datos y no se sincroniza con ninguno.

Como en toda inhibición la diferencia está en cuanta potencia se utiliza para inhibir, esta técnica es muy eficiente en potencia ya que no transmitimos continuamente y solo hace falta transmitir un poco por encima de la potencia con que recibe el terminal móvil a la estación base.

En el siguiente apartado demostraré la relación más eficiente en cuanto a la potencia nominal del FCCH interferente y el número de FCCHs interferentes que vamos a enviar.

4.3 Resultados en simulación.

Lo primero que se necesita para simular un inhibidor, es simular un sistema de comunicaciones, la herramienta que vamos a utilizar para ello es Matlab.

Primero vamos a simular un emisor el cual envía la multi – trama 51 modulada y un receptor que la demodule y reciba. Para ello la lógica de secuencias que hemos seguido ha sido la siguiente: Generar las tramas a nivel más bajo (las de 156 bits) del FCCH, BCCH, SCH y CCCH, después modularlas con una GMSK y montarlas en la multi – trama 51, simular que se envía al receptor y éste separa la multi – trama 51 y demodula los diferentes canales.

A continuación las figuras de los canales modulados en tiempo y en frecuencia.

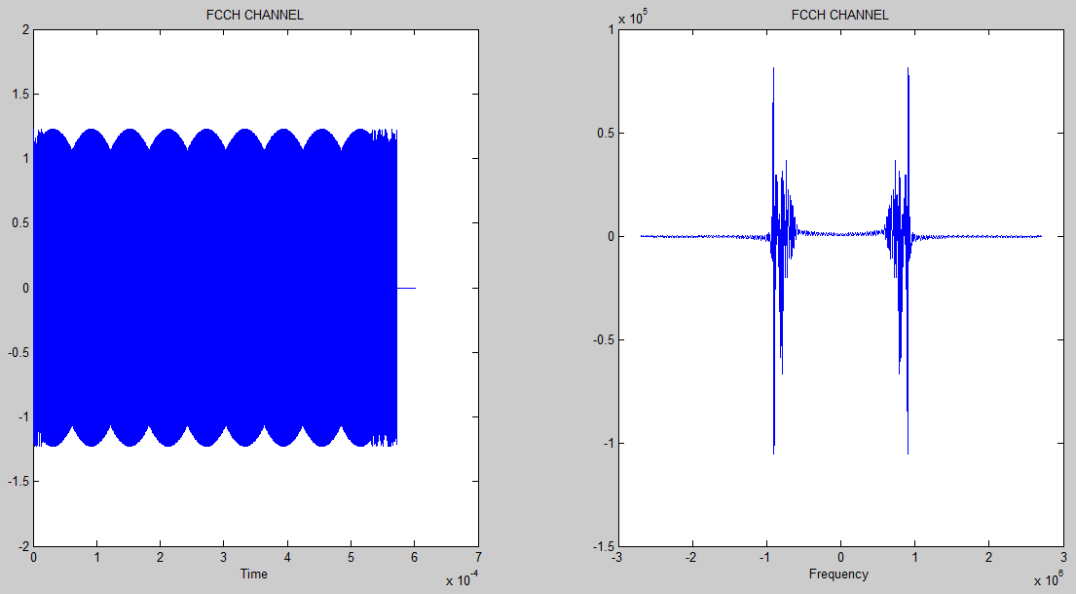

Figura 4.5, FCCH modulado en tiempo y en frecuencia.

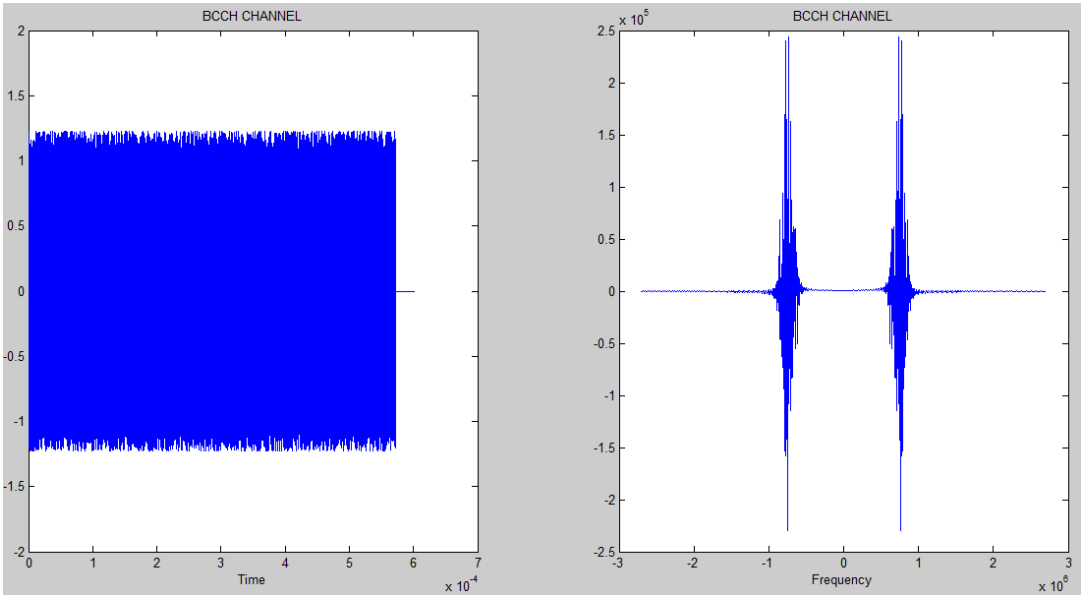

Figura 4.6, BCCH modulado en tiempo y en frecuencia.

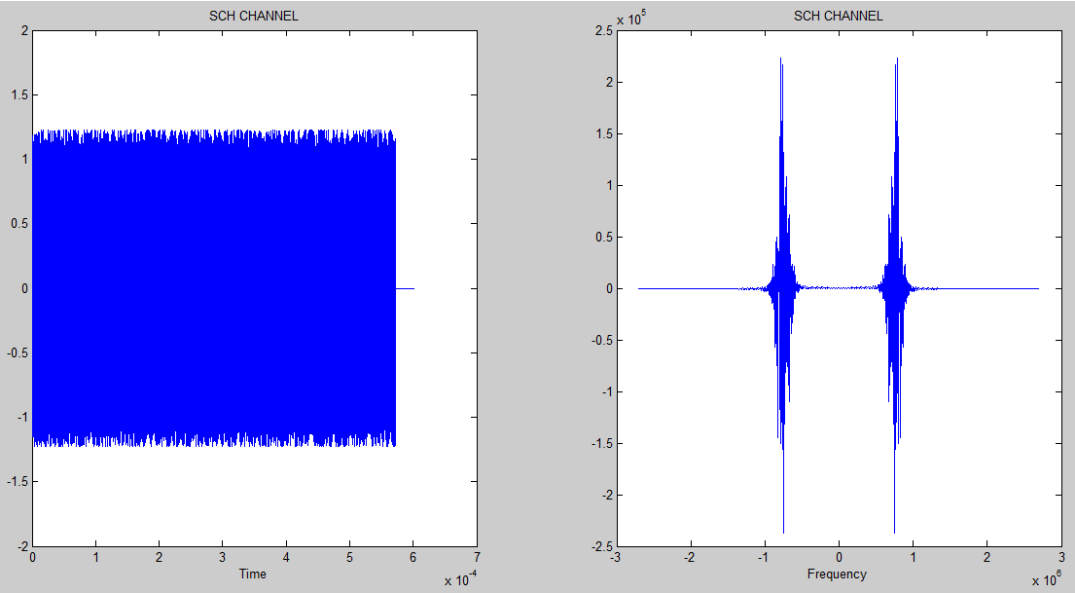

Figura 4.7, SCH modulado en tiempo y en frecuencia.

De estos canales el que más nos interesa es el FCCH ya que lo tenemos modulado y es el que vamos a utilizar para inhibir.

Cuando ya tenemos todos los canales modulados lo que tenemos que hacer ahora es construir la multi – trama 51 ya que sobre ella es sobre la que vamos a hacer las pruebas de inhibición, simulando que la multi – trama 51 construida es la enviada por la estación base.

El siguiente paso consiste en encontrar la mejor relación entre el tamaño en potencia de nuestro FCCH interferente y la cantidad de ellos que tenemos que enviar. Para ello vamos a valernos del cálculo de la SIR cuya fórmula es la siguiente:

$$SIR = \frac{Potencia\ \ del\ FCCH\ normal}{Potencia\ \ del\ FCCH\ interferente} \qquad (4.2)$$

La finalidad de esto es calcular el error que hay entre la interferencia del FCCH interferente y el FCCH normal en función de la SIR para encontrar la relación de potencia más favorable. En comunicaciones se considera un error del 10% como suficiente para considerar inhibición. La fórmula utilizada para calcular el error en Matlab es la siguiente, que corresponde al error cuadrático medio.

$$ERROR = mean\ ((FCCH\_normal) - (FCCH\_interferente(i)))\text{.}\hat{}2 \qquad (4.3)$$

Para realizar estos cálculos basta con calcular en bucle los errores de los distintos FCCHs interferentes superpuestos al FCCH normal. Con la siguiente imagen lo observaremos con facilidad.

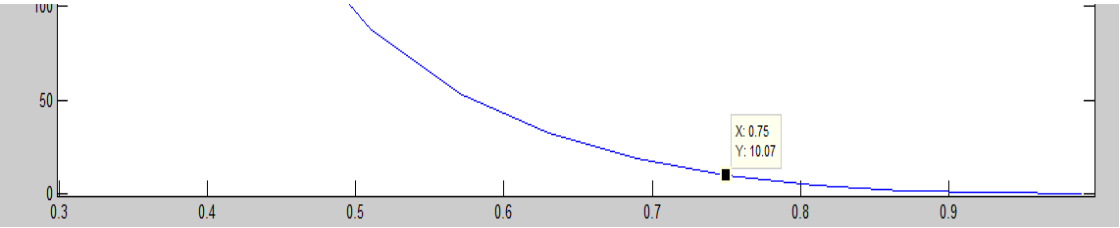

Figura 4.8, Error en función de SIR.

La figura es una exponencial decreciente de manera que conforme la potencia del FCCH interferente se acerca a la potencia nominal del FCCH normal, el error se acerca al nulo.

Se observa en la figura que el límite del 10% se atraviesa cuando SIR = 0.75, es decir, cuando la potencia del FCCH interferente es de 1.33 periódico puro, por lo que vamos a establecerlo en 1.34.

Una vez establecido el tamaño en potencia del FCCH interferente con respecto del FCCH normal, hay que probar el número de FCCHs interferentes que sea el más eficaz y en qué parte de la multi – trama 51. Para ello, hemos desarrollado un programa que calcula bit a bit el error de un FCCH interferente con 1.34 veces la potencia del FCCH normal superpuesto en todos los slots, después lo mismo con dos FFCHs interferentes y después con tres y así sucesivamente hasta llegar a alcanzar un tamaño de 0.17 veces el tamaño de la multi – trama 51.

El 0.17 es un número obtenido mediante otra figura en la que comparamos el error resultante en función del número de FCCHs interferentes que utilizamos, puesto que no podemos estar emitiendo FCCHs interferentes todo el tiempo que dura la multi – trama 51 porque produciría mucho gasto en potencia, hemos decidido transmitir como mucho el 17% del tiempo, es decir, unos 40 ms. En la siguiente figura observamos que la gráfica es ascendente como era de esperar ya que cuantos más FCCHs interferentes mayor error vamos a obtener. El 17% se encuentra en 27 tramas ya que 27 es el 17% de 156.

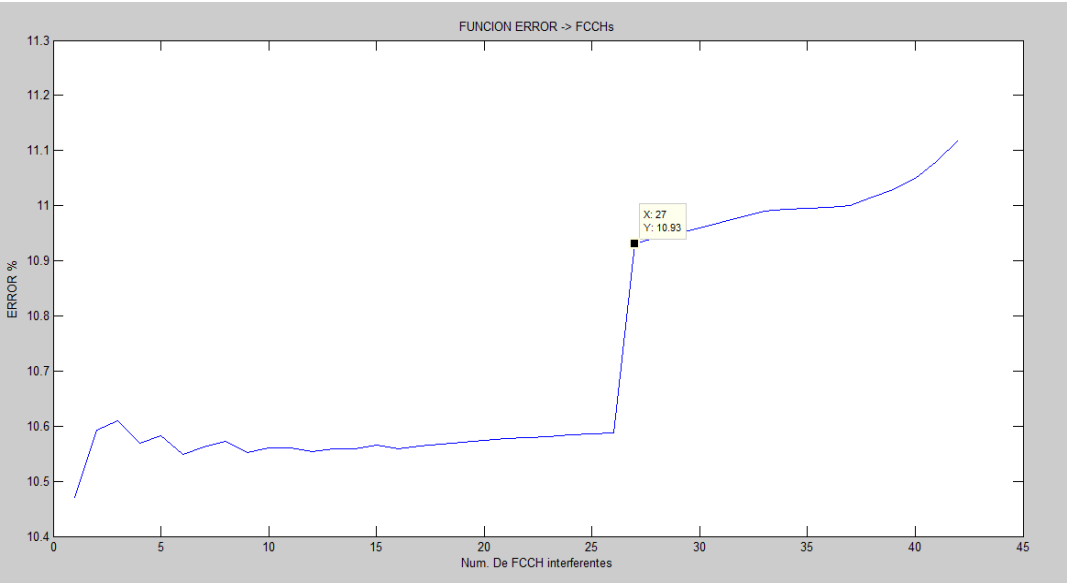

Figura 4.9, Error en función del número de FCCHs interferentes utilizados.

En la figura anterior se observa como todos los errores parten por encima del 10% puesto que estos cálculos se han hecho contando ya con un FCCH interferente de 1.34 veces la potencia del FCCH normal. El hecho de que haya un salto a partir de unos 26 FCCHs interferentes se debe a que una vez atravesado este límite, la secuencia interfiere con dos canales FCCH y dos canales SCH, fenómeno que apreciaremos en la siguiente figura. De esta forma la secuencia siempre coincidirá con algún canal de control aún sin conocer los tiempos en los que transmite la estación base.

Esto en la práctica no se puede implementar correctamente debido a que no se sabe con exactitud el momento en el que empieza a transmitir la estación base por lo que este resultado es meramente teórico.

En la siguiente figura mostramos diferentes ejemplos en los que nuestra secuencia de 27 FFCHs interferentes podría interferir. Por supuesto hay 129 casos diferentes en los que nuestra secuencia puede empezar a coincidir con la multi – trama 51, pero solo escenificaremos un caso.

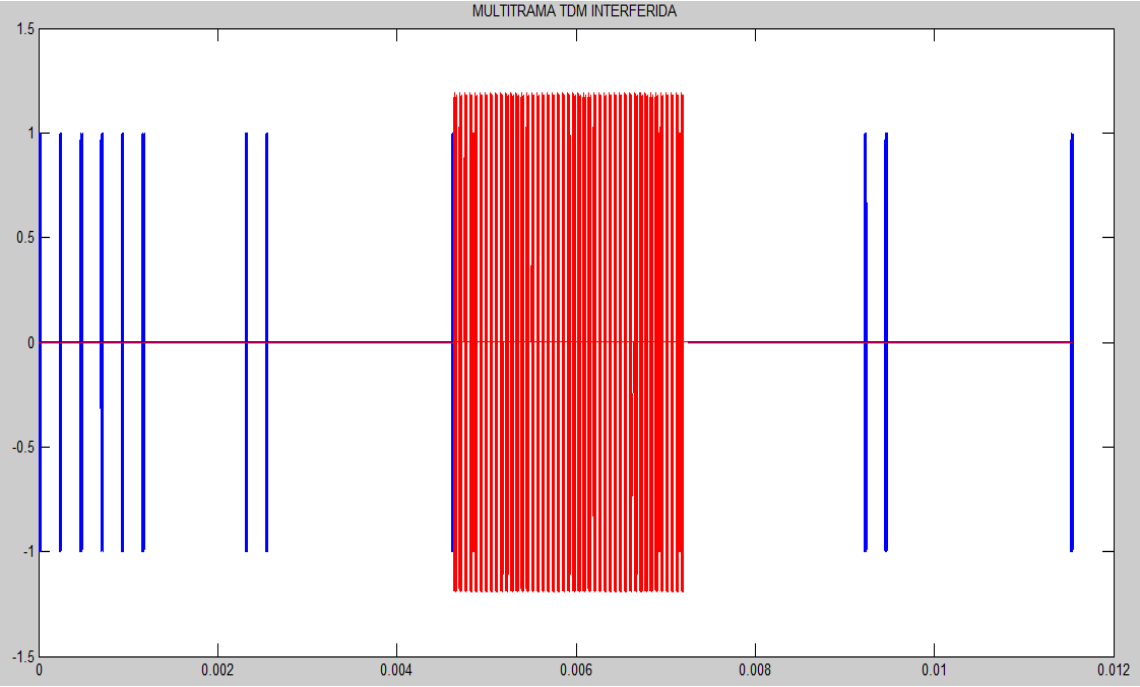

Figura 4.10, Multi – trama 51 interferida por la secuencia interferente.

En rojo tenemos la secuencia de FCCHs interferentes y en azul la multi – trama 51. Las partes nulas corresponden a los slots de los canales CCCH los cuales no necesitamos incluir en la simulación puesto que nuestro objetivo es principalmente inhibir a los canales FCCH, BCCH y SCH.

Con todos estos datos se concluye que la forma más eficiente de inhibir consiste en enviar una secuencia de 27 FCCHs interferentes a una potencia 1.34 veces mayor de la que el terminal móvil recibe de la estación base.

4.4 Resultados prácticos.

Para traducir esto a la práctica necesitamos las siguientes herramientas:

• National Instruments USRP 2920.

• Analizador vectorial.

• Un ordenador, en este caso el mio: Sony Vaio serie SVE.

• Software: Lab View student edition.

• Cable Ethernet de 1 Gb.

• Antena de transmisión.

• Cargador del USRP2920.

Una vez contamos con todas las herramientas procedemos a inhibir. Para inhibir conectamos la antena al USRP 2920, y éste a la red de alimentación con el cargador. Conectamos el USPR 2920 al ordenador mediante el cable Ethernet de 1 Gb y a través de Lab View emitimos nuestra secuencia interferente, la cual es recogida por el analizador vectorial. Con el analizador vectorial somos capaces de ver en tiempo y en frecuencia, las tramas de GSM que se transmiten y por lo tanto para ver si inhibimos correctamente tenemos que observar distorsión en dichas tramas.

Otra forma más eficaz de saber si estamos inhibiendo consiste en hacer utilizar a un teléfono cualquier la red GSM (2G) y conociendo la frecuencia a la que el operador del teléfono opera en GSM podemos inhibir en la misma frecuencia de manera que se observe que efectivamente el teléfono móvil es incapaz de conectarse a la red.

Para lograr esto en Lab View hemos tenido que desarrollar un modelo circuital que sea capaz de enviar dicha secuencia interferente.

En primera instancia desarrollamos el circuito de la modulación GMSK para poder modular nuestro FCCH interferente, para ello nos hemos servido de un filtro gaussiano y una MSK. En la siguiente figura se observa nuestro FCCH interferente modulado y la constelación de la GMSK.

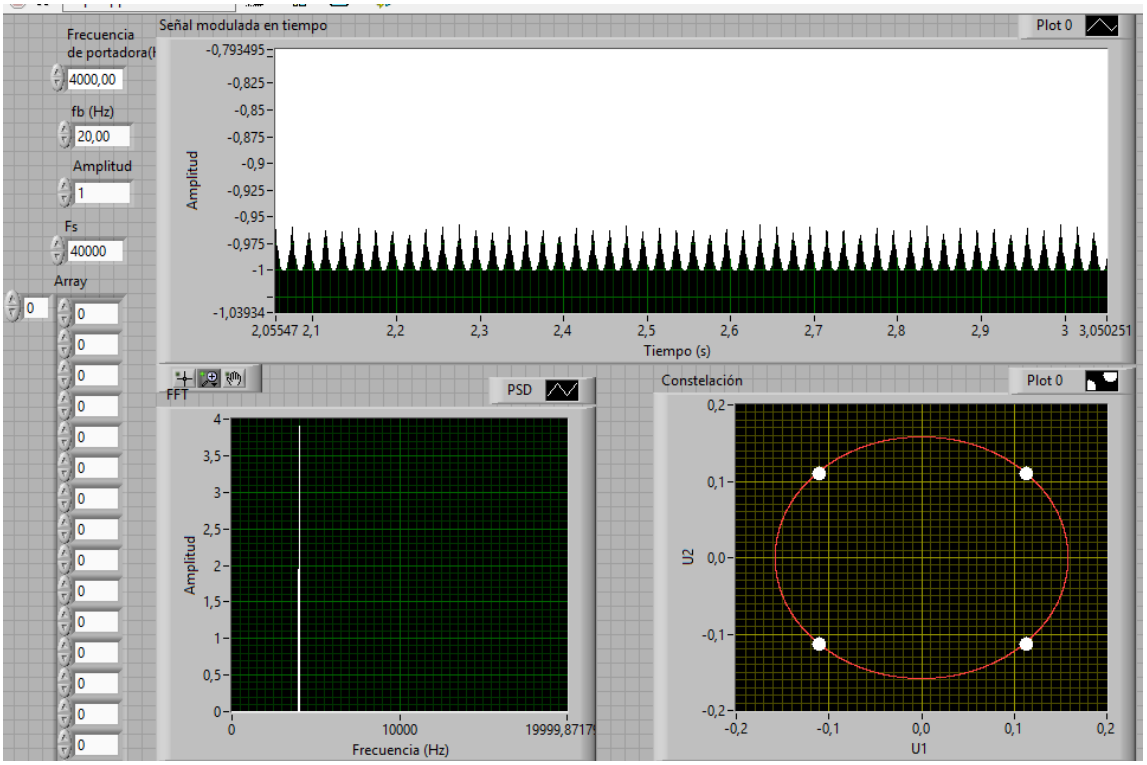

Figura 4.11, FCCH modulado con GMSK y su constelación.

Como vemos en la figura, la similitud del FCCH modulado en tiempo en la práctica y en la simulación es muy similar, al igual que la figura teórica de la GMSK y la que hemos obtenido en la figura.

Por otro lado podemos comenzar a utilizar el analizador vectorial para poder observar la red GMS, su constelación y sus tramas. Para ellos configuramos el analizador vectorial como demodulador digital para la red GSM y buscamos las frecuencias en las que se utiliza esta red. En la siguiente tabla podemos observar qué frecuencias utilizan qué operadores en España.

FRECUENCIAS UTILIZADAS POR LAS OPERADORAS EN ESPAÑA PARA GSM

Operadoras	**Uplink MHz**	**Downlink MHz**
Movistar	890 - 905	935 - 950
Movistar	1710 - 1730	1805 - 1825
Orange	880 - 890	925 - 935
Orange	1765 - 1785	1860 - 1880
Vodafone	900 - 915	950 - 960
Vodafone	1730 - 1750	1825 - 1845
Yoigo	1750 - 1765	1845 - 1860

Tabla 4.1, Frecuencias utilizadas por las operadoras en España para GSM.

En este caso como pertenezco a Movistar, y nosotros queremos observar los canales de control, tendremos que coger una frecuencia de Movistar del enlace de bajada, por ejemplo 935 MHz.

Escogemos dichos parámetros en el analizador vectorial para observar las características de la red GSM recogidas en la siguiente figura.

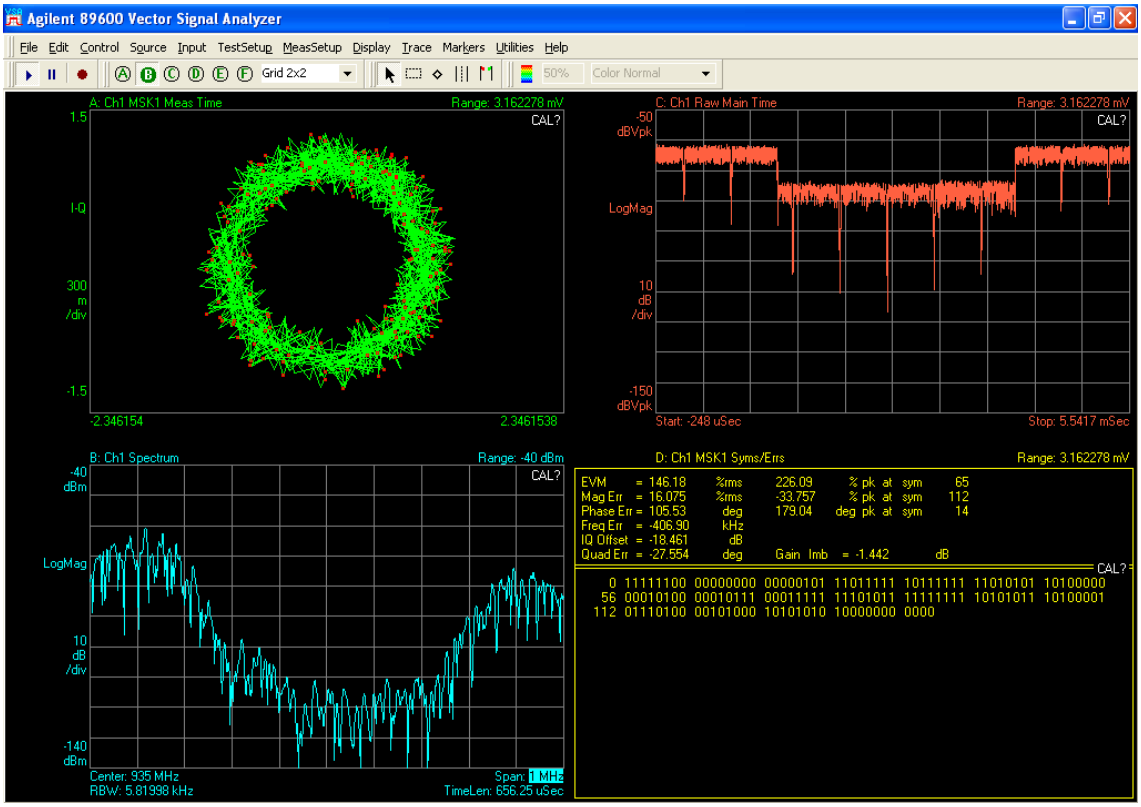

Figura 4.12, Red GSM capturada desde el analizador vectorial.

Arriba a la izquierda de la imagen observamos la constelación GMSK más o menos nítida, arriba a la derecha observamos en el tiempo las tramas de GSM. Abajo a la izquierda observamos el espectro y abajo a la derecha la codificación a nivel de bit con diferentes parámetros para identificar el error.

El analizador vectorial está calibrado a -40 dBm porque es más o menos la sensibilidad necesaria para observar la red GSM, si lo calibramos más bajo se satura el analizador y si lo ponemos más alto no se observaría correctamente los elementos de la red GSM.

El siguiente paso del analizador vectorial consistirá en observar la inhibición creada por nuestro inhibidor, por lo que de momento lo dejamos como está. Ahora mismo tenemos el analizador vectorial listo, y nuestro FCCH interferente también. Solo queda crear una trama de tamaño 3 slots. Esto se debe hacer porque como hemos dicho antes en simulación, nosotros lo que queremos es enviar el FCCH interferente, pero no de manera continua en todos los slots de la multi – trama 51, ya que eso sería un gasto muy alto de potencia. Lo que haremos entonces es construir la trama de 3 slots de manera que los tendremos colocados de la siguiente forma: FCCH interferente, slot vacío, slot vacío. De esta forma si enviamos esta trama de forma continua durante el tiempo calculado en las simulaciones (40 ms de inhibición por cada multi – trama 51) obtendremos nuestra trama completa interferente, por supuesto tendremos que enviar varias secuencias interferentes ya que la estación base no envía una única multi – trama51.

En la siguiente figura mostramos el panel resultante del circuito que genera nuestra secuencia interferente.

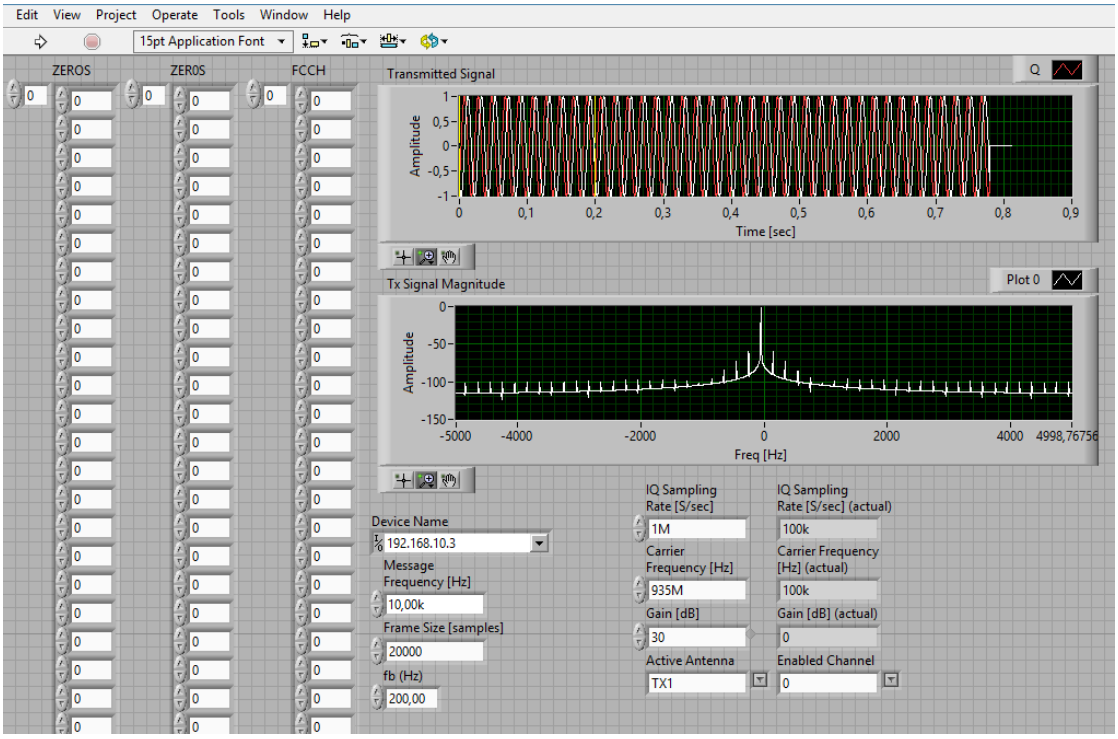

Figura 4.13, Panel de control del circuito inhibidor.

En esta figura podemos observar los arrays creados para el FCCH interferente y los dos slots vacíos, aparentemente son iguales pero la diferencia está en que el FCCH pasa por un modulado mediante la GMSK la cual generará una sinusoide y los otros dos no.

En la parte inferior derecha tenemos los parámetros de control, donde controlamos la dirección IP del USRP 2920, la frecuencia de portadora, la ganancia con la que emitimos, la antena por la que transmitimos, tasa de bit, frecuencia del mensaje y tamaño del mensaje.

En la parte superior derecha tenemos unos gráficos representativos de lo que estamos enviando, el gráfico superior muestra nuestra trama en tiempo y el inferior en frecuencia.

Pues bien, una vez lo tenemos todo solo nos queda inhibir, para ello corremos nuestro programa para emitir la secuencia interferente. Para observar la inhibición vamos a utilizar mi teléfono, vamos a forzarlo para funcionar en la red 2G, GSM. Esto se puede realizar de manera sencilla desde los ajustes del teléfono.

Para saber si estamos inhibiendo o no hemos descargado una aplicación que nos da ciertos detalles sobre el CID de la estación base a la que estamos conectados. La aplicación se llama Network Cell Info Lite y la siguiente figura muestra la interfaz de esta aplicación. En dicha interfaz podemos observar que estamos funcionando en GSM y que la estación base con CID 5541 es la que nos está prestando servicio, el resto de estaciones aparecen como vecinos más cercanos a los que se conectaría el teléfono en caso de perder la señal con la estación base 5541.

Figura 4.14, Interfaz de la aplicación Network Cell Info Lite (versión gratutita).

Por desgracia ninguna aplicación ha sido capaz de mostrarnos la frecuencia en la que transmite la estación base a la que estamos conectados por lo que hemos tenido que ir probando a inhibir todas las frecuencias GSM de Movistar hasta dar con la frecuencia a la que transmite la estación base con CID 5541. Como resultado hemos hallado la frecuencia de 935,8 MHz.

En esta frecuencia hemos conseguido inhibir la estación base de CID 5541 para que deje de prestarnos servicio, como consecuencia el teléfono salta a otra estación base. Hemos comprobado que al reiniciar la búsqueda del teléfono de una red a la que conectarse como por ejemplo, conectar y desconectar el modo avión y apagar el inhibidor, el teléfono vuelve a conectarse a la estación base de CID 5541 y si volvemos a activar el inhibidor vuelve a perder su señal y saltar de frecuencia.

Hemos comprobado el funcionamiento del inhibidor para diferentes tramas a diferentes potencias. En el primer caso probamos a transmitir continuamente un FCCH interferente, siendo la mínima potencia necesaria para inhibir de 25 dB. En el segundo caso hemos probado a inhibir con una secuencia como la que hemos generado en la teoría, en este caso no hemos conseguido inhibir ni al máximo de la potencia que permite el USRP 2920 la cual es de 31 dB. En vista de esto hemos decidido aumentar la presencia del FCCH interferente y en este tercer caso enviamos por cada slot vacío, dos FCCHs interferentes (antes era al revés) y sí hemos conseguido inhibir hasta un mínimo de 27 dB de ganancia.

5. MARCO REGULADOR

5.1 Leyes que proceden.

Tal y como hemos mencionado antes en el punto 2, el uso de estos aparatos está restringido a las fuerzas de seguridad del estado y al ejército que son los organismos que usan estos inhibidores de frecuencia, con el fin de evitar ataques remotos ya sea por ondas de radio, drones o explosivos remotos. Por este motivo al aproximarnos a una comisaría de policía o cuartel militar es normal que los aparatos como los móviles no nos funcionen, de la misma forma si nuestro coche está aparcado cerca de un coche oficial el cual lleva un inhibidor de frecuencias podemos observar como la llave para abrir a distancia nuestro coche no funciona.

Legalmente las leyes aplicables que tienen en relación al uso de inhibidores de frecuencias son las siguientes, en las cuales citaré párrafos de algunas de ellas;

• Directiva de la Comisión Europea 99/05/CE

" Los equipos radioeléctricos cuya puesta en servicio sea objeto de restricciones por los Estados miembros, según lo previsto en el apartado 2 del artículo 7 de la Directiva 1999/05/CE, o cuya puesta en el mercado esté limitada según lo previsto en el apartado 5 del artículo 9 de la Directiva 1999/05/CE, constituirán una categoría. Dicha categoría se denominará categoría 2." [10].

• Real Decreto 1890/2000 de 20 de noviembre por el que se aprueba el procedimiento para la evaluación de la conformidad de los aparatos de telecomunicaciones.

"Si los equipos anulan las frecuencias de radio mediante la emisión de señales radioeléctricas que perturbando, crean interferencias que inhabilitan, por ejemplo, el uso de teléfonos móviles, estos equipos, por el solo hecho de utilizar el espectro radioeléctrico, deberán estar a lo dispuesto en la Directiva 99/05/CE, transpuesta a la legislación española mediante el Real Decreto 1890/2000 de 20 de noviembre" [9].

• Informe de la Secretaría de Estado de Telecomunicaciones de fecha 28 de diciembre de 2004.

• Título VIII de la Ley 32/2003 de 3 de noviembre, General de Telecomunicaciones. Artículos de inspección y régimen sancionador. Artículos 50-55.

• Decisión de la Comisión de 6 de abril de 2000 relativa al establecimiento de la clasificación inicial de los equipos radioeléctricos y equipos terminales de telecomunicación y los identificadores asociados.

• Decisión de la Comisión de 26 de julio de 2002 por la que se crea un Grupo de política del espectro radioeléctrico.

• Decisión nº 676/2002/CE del Parlamento Europeo y del Consejo sobre un marco regulador de la política del espectro radioeléctrico en la Comunidad Europea.

“El objetivo de la presente Decisión es establecer en la Comunidad un marco político y jurídico que asegure la coordinación de los planteamientos políticos y, en su caso, las condiciones armonizadas que permitan la disponibilidad y el uso eficiente del espectro radioeléctrico necesarios para el establecimiento y funcionamiento del mercado interior en ámbitos de políticas comunitarias como las comunicaciones electrónicas, los transportes, y la investigación y el desarrollo (I+D)”. [8]

Y por último el Comité de Vigilancia del Mercado y evaluación de la conformidad en materia de Telecomunicaciones (TCAM), del que emana la Directiva, y mediante el cual se ha llegado a un acuerdo, entre todos los Estados miembros, de no autorizar este tipo de equipos, salvo las excepciones previstas en la norma en el ámbito de la seguridad pública.

“ No obstante, debe tenerse en cuenta que la Directiva contempla una serie de equipos que están exentos de la aplicación de la misma, como pueden ser los utilizados, exclusivamente, para actividades relacionadas con la seguridad pública, la defensa nacional, la seguridad del estado y las actividades del Estado en el ámbito del Derecho Penal. De ello se deduce que, en determinadas circunstancias, estos equipos pueden ser puestos en servicio, siempre que se encuentren en la situación anterior, ya que no les sería de aplicación ni la Directiva ni el Real Decreto”. [7]

Estas leyes, decretos y decisiones existen para regular no solo este tipo de aparatos si no también el espectro radioeléctrico. La principal causa de por qué estos aparatos están regulados es por el uso delictivo que se les puede dar así como la interrupción del espectro radioeléctrico en un cierto espacio.

5.2 El mal uso de los inhibidores de frecuencia.

Los inhibidores de frecuencias tienen ciertos usos que van de la mano de delitos penados por la ley. El caso es que estos equipos se pueden utilizar para inhibir cualquier tipo de señal, desde una alarma de una casa o una tienda que funcione por radiofrecuencia hasta interferir en equipos de la policía o en equipos privados con el fin de evitar algún tipo de comunicación. Pongamos el ejemplo de un tipo de alarma como la alarma que se sirve del espectro radioeléctrico para transmitir, estas alarmas comunican lo que sucede dentro del recinto protegido a través de un modulo de comunicación que transmite audio y video a la empresa protectora, y cualquier persona con un inhibidor puede anular completamente este sistema de alarma.

Hoy en día es fácil encontrar por internet distintos tipos de inhibidores según su potencia, frecuencia, alcance, función, uso y a diferentes precios. Pongo por ejemplo a disposición una serie de inhibidores cuyo precio y capacidad van desde los 100 euros inhibiendo la red GSM en unos pocos metros hasta los 20 mil euros inhibiendo cualquier frecuencia a varios cientos de metros de distancia.

• TX166 – Inhibidor Portátil. Éste es un inhibidor portátil del tamaño de un libro de bolsillo, capaz de inhibir en GSM, 3G, 4G LTE, WIFI, BLUETOOTH y sobrando un antena para inhibir una frecuencia personalizada. Pesa menos de 2 kilogramos con una

potencia de unos 7W con un alcance de entre 5 y 30 metros por un precio de 559 Euros. Éste inhibidor es más que suficiente para eliminar una alarma.

Disponible en: (http://www.projammers.com/es/home/tx166-inhibidor-portatil.html) [4]

• HDT-960 Desktop Drone RF Jammer 8 Bands 2.4 GHz+GPS+5.8 GHz. Un inhibidor que anula señal GPS, específico para drones con alcance de 40 metros por 881.89 Euros.

Disponible en: (https://www.perfectjammer.com/low-power-desktop-drone-jammers-8-bands.html) [5]

•Inhibidor portátil de cobertura para móviles. Éste inhibidor podríamos decir que es el más sencillo del mercado, inhibe solo GSM con un radio efectivo de 3 metros de distancia y una potencia de 200mW. Tiene un precio de 129.10 Euros. Disponible en: (https://www.solostocks.com/venta-productos/antenas/antenas-telefonia-movil/inhibidor-portatil-de-cobertura-para-moviles-4180201). [6]

•TX101M NET – Inhibidor de frecuencias. Éste inhibidor tiene el tamaño de un mueble pequeño, capaz de inhibir en GSM, 3G, 4G LTE, WIFI, BLUETOOTH, GPS. Tiene una potencia de entre 200W y 400W y un radio de 500 metros, lo cual le hace perfecto para cuarteles militares o complejos gubernamentales. Tiene un precio de 23.500 Euros. Disponible en:

(http://www.projammers.com/es/home/tx101m-net-inhibidor-de-frecuencias.html). [4]

Es por ello que estos sistemas están prohibidos con sus diferentes excepciones ya mencionadas anteriormente y su uso indebido achaca una serie de sanciones personales y jurídicas.

5.3 Sanciones.

Previamente a la sanción se lleva a cabo una inspección de los servicios y de las redes de telecomunicaciones, de sus condiciones de prestación, de los equipos, de los aparatos, de las instalaciones y de los sistemas civiles por parte del organismo competente. Dicho organismo competente contará con un servicio central de inspección técnica de telecomunicaciones y de la del Mercado de las Telecomunicaciones, la cual podrá controlar e inspeccionar las actividades de los operadores de telecomunicaciones, sin embargo será únicamente potestad del Ministerio competente la imposición de sanciones.

Por otro lado el control e inspección del dominio público radioeléctrico corresponde a la Agencia Estatal de Radiocomunicaciones siendo posible en ciertos casos que el Ministerio competente o la Comisión del Mercado de las Telecomunicaciones, en materias de su competencia, podrán solicitar la actuación de la Agencia Estatal de Radiocomunicaciones.

Existen diferentes tipos de sanciones función y rangos entre los que la sanción a aplicar se decide por los siguientes motivos:

• La gravedad de las infracciones cometidas anteriormente por el sujeto al que se sanciona.

• La repercusión social de las infracciones cometidas.

• El beneficio que haya reportado al infractor el hecho objeto de la infracción

• El daño causado.

Y éstas se catalogan de mayor a menor sanción por: muy grave, grave y leve. Para las cuales existen distintas sanciones.

"Por la comisión de infracciones muy graves tipificadas en los párrafos q) y r) del artículo 53 del Título VIII de la Ley 32/2003 de 3 de noviembre, General de Telecomunicaciones, se impondrá al infractor multa por importe no inferior al tanto, ni superior al quíntuplo, del beneficio bruto obtenido como consecuencia de los actos u omisiones en que consista la infracción. En caso de que no resulte posible aplicar este criterio o que de su aplicación resultara una cantidad inferior a la mayor de las que a continuación se indican, esta última constituirá el límite del importe de la sanción pecuniaria. A estos efectos, se considerarán las siguientes cantidades: el uno por ciento de los ingresos brutos anuales obtenidos por la entidad infractora en el último ejercicio en la rama de actividad afectada o, en caso de inexistencia de éstos, en el ejercicio actual: el cinco por ciento de los fondos totales, propios o ajenos, utilizados en la infracción, o 20 millones de euros". [17]

Las infracciones muy graves, en función de sus circunstancias, podrán dar lugar a la inhabilitación hasta de cinco años del operador para la explotación de redes o la prestación de servicios de comunicaciones electrónicas.

Por lo que es una opción seriamente a tomar no cometer este tipo de infracción, un ejemplo de lo que se considera como infracción muy grave es el uso, en condiciones distintas a las autorizadas, del espectro radioeléctrico que provoque alteraciones que impidan la correcta prestación de otros servicios por otros operadores.

Por la comisión de infracciones graves se impondrá al infractor multa con el límite máximo de 500.000 euros.

Las infracciones graves, en función de sus circunstancias, podrán llevar aparejada amonestación pública, con publicación en el "Boletín Oficial del Estado" y en dos periódicos de difusión nacional, una vez que la resolución sancionadora tenga carácter firme.

Por la comisión de infracciones leves se impondrá al infractor una multa por importe de hasta 30.000 euros.

Las infracciones leves, en función de sus circunstancias, podrán llevar aparejada una amonestación privada.

6. ENTORNO SOCIO-ECONÓMICO

6.1 Presupuesto.

Para este proyecto hemos calculado el siguiente presupuesto:

TABLA DE PRESUPUESTO

Elementos utilizados	**Precio**
Analizador Vectorial (amortizado su uso a 2 mes)	2.000 €
National Instruments USRP 2920 (amortizado su uso a 2 meses)	101,6 €
Sony Vaio serie SVE (amortizado su uso a dos meses)	50 €
Trabajo del alumno (6 meses)	8.400 €
Trabajo del profesor (6 meses)	14.400 €
Gastos indirectos 20% del total (sin IVA)	4.990,32 €
Presupuesto total (sin IVA)	29.941,92 €
Presupuesto total (con IVA)	36.229,72 €

Tabla 6.1, Presupuesto del proyecto.

6.2 Impacto socio-económico.

El desarrollo de este proyecto, un inhibidor de frecuencias de la red GSM en tecnología de radio definida por software tiene un impacto social en relación a la seguridad, la libertad y la salud.

En cuanto a la seguridad, que va de la mano de la salud, como hemos mencionado en apartados anteriores los inhibidores están reservados a fuerzas de seguridad del Estado porque son un elemento que sirve para defenderse de posibles ataques. Por ejemplo, parte del ejército está desplegado en Bagdad o en cualquier otra zona conflictiva, en una base en medio de la nada pueden ser perfectamente objetivos de ataques terroristas con bombas por control remoto o incluso en función de la tecnología de la que dispongan el o los atacantes pueden llegar a utilizar drones de combate. El simple hecho de que esa base militar en medio de la nada tenga un inhibidor de frecuencias puede salvarle la vida a la mayoría de soldados que podrían haber sido objetivo del ataque.

Incluso si pensamos en la guerra, uno de los principales objetivos en una guerra se considera el evitar que los enemigos se comuniquen entre ellos. En la antigüedad para hacer esto se hacían movimiento de pinza sobre el terreno de mantera que se separaba al grupo enemigo en dos o más grupos pequeños de manera que el general en alguno de esos grupos no podía comunicar qué hacer a sus soldados. En las guerras modernas como la primera o la Segunda Guerra Mundial como ya existían las radiocomunicaciones pero no eran tas sofisticadas como para tener inhibidores funcionales, la victoria erradicaba no en evitar que el enemigo se comunicase si no en descifrar los códigos del enemigo para conocer los planes de ataque.

Por otro lado la existencia de estos inhibidores obligará a los futuros atacantes a intentar desarrollar tecnología anti – inhibidores que incluso algunos ya existen en forma de alarmas anti – inhibidores y se pueden comprar por internet.

Siendo un poco menos melodramáticos, esta tecnología en el momento en que no afecta a la seguridad o a la salud, puede afectar fácil y sencillamente a nuestra libertad. El ejemplo más sencillo podría ser un simple vecino o un desconocido mal intencionado, que desea dejarnos incomunicados por cualquier razón, o simplemente el hecho de acercarnos a un coche oficial o a un cuartel de policía y no poder utilizar el teléfono, o no poder abrir el coche con el mando a distancia, algo que en ocasiones ocurre y mucha gente no tiene conocimiento de que en realidad se trata de un inhibidor de frecuencias, y puede llegar a pensar que o su teléfono móvil o sus llaves del coche no funcionan apropiadamente. También un ladrón puede utilizar un inhibidor para inhibir nuestra alarma y después volver a utilizarlo para inhibir nuestra telefonía móvil de tal manera que puede en un momento dejarnos sin seguridad y sin comunicaciones.

En cuanto al impacto económico hemos hablado de guerra, ladrones en casas, y atentados terroristas. Como saben todo esto está ligado a una gran cantidad de dinero ya sea por intentar prevenir cualquier atentado terrorista o por intentar evitar que roben en casa, a pequeña o grande escala esta tecnología lleva a la gente a desembolsar cantidades altas de dinero con el fin de defenderse. Ya hemos observado el precio de alguno de estos inhibidores y por el otro lado de la economía el número de empresas que se dedican a crear, vender y distribuir esta tecnología está aumentando y más empresas con esta tecnología implica más competitividad y más competitividad implica desarrollo. Por otro lado cabe resaltar las estadísticas económicas en números y que mencionamos en el punto 3.3. En 2017 las tecnologías y servicios de telefonía móvil generó el 4.5% del PIB del mundo, una valoración de 3.6 billones de dólares. Se han generado alrededor de 29 millones de puestos de trabajo directa o indirectamente por todo el mundo y ha enrriquecido el sector público en 500 mil millones de dólares en impuestos y a través de subastas del espectro radioeléctrico. Como se observa este sector ha generado mucha riqueza y puestos de trabajo, por lo que merece la pena todo lo que tenga que ver con el ya sea un inhibidor o un nuevo sistema de comunicación.

Por lo que en definitiva el impacto social de esta tecnología es tanto positivo como negativo en aspectos de seguridad y salud, por supuesto positivo económicamente

hablando ya que toda tecnología produce dinero y por último negativo en términos de libertad ya que nuestra capacidad de conexión se puede ver alterada sin necesidad ni de saber que estamos ante un inhibidor de frecuencias.

Como toda tecnología nueva que nace el hecho de que existan estos inhibidores y anti inhibidores lleva al ser humano a en el futuro desarrollar inhibidores y anti inhibidores mucho más sofisticados al igual que los sistemas que inhiben. El ciclo de la vida de la tecnología consiste en alimentarse de sí misma para seguir evolucionando.

7. BLIBIOGRAFÍA

[1] Yossef Gofman Ofer Yarden-Zaslavsky, “Electronic device and method og blocking cellular communitacion”, patente, propiedad de: Netline Communications Tech NCT Ltd, Estados Unidos, 26/11/1996. Disponible en: https://patents.google.com/patent/US6456822. 15/09/2018.

[2] 陈道民 陆贻东, “Omnibearing seeking multi-frequency wave inhibitor”, patente, propiedad de: 陆贻东, China, 21/03/2001. Disponible en: https://patents.google.com/patent/CN2424581Y/en?oq=frequency+inhibitor. 15/09/2018.

[3] Víctor P. Gil Jiménez, Ana García Armada, Nieves Sidney González Pizarro, Francisco Hernando Gallego, "Método y dispositivo para la inhibición de señales de telefonía móvil", patente, propiedad de: Universidad Carlos III de Madrid, España, 13/09/2012. Disponible en: http://invenes.oepm.es/InvenesWeb/detalle?referencia=P201231410. 15/09/2018.

[4] Venta de inhibidores portátiles y fijos por internet. Disponible en:

http://www.projammers.com/es/home/tx166-inhibidor-portatil.html. 09/09/2018.

[5] Venta de inhibidores de drones por internet Disponible en:

https://www.perfectjammer.com/low-power-desktop-drone-jammers-8-bands.html. 09/09/2018.

[6] Venta de inhibidor simple por internet. Disponible en:

https://www.solostocks.com/venta-productos/antenas/antenas-telefonia-movil/inhibidor-portatil-de-cobertura-para-moviles-4180201. 09/09/2018.

[7] E.Gándara Trueba, “Inhibidores de frecuencia”, Ministerio del Interior, España, INFORME UCSP Nº: 2010/009, 16/02/2010. Disponible en:

https://www.policia.es/org_central/seguridad_ciudadana/unidad_central_segur_pri/i_reservada/2010/2010_009.pdf 05/09/2018.

[8] Decisión nº 676/2002/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, sobre un marco regulador de la política del espectro radioeléctrico en la Comunidad Europea (Decisión espectro radioeléctrico), Comunidades Europeas, Bruselas. DOUE-L-2002-80697. Disponible en: https://www.boe.es/buscar/doc.php?id=DOUE-L-2002-80697 05/09/2018.

[9] Real Decreto 1890/2000, de 20 de noviembre, por el que se aprueba el Reglamento que establece el procedimiento para la evaluación de la conformidad de los aparatos de

telecomunicaciones, Ministerio de Ciencia y Tecnología, España, BOE-A-2000-21838. Disponible en:

https://www.boe.es/buscar/doc.php?id=BOE-A-2000-21838 05/09/2018.

[10] Directiva 1999/5/CE del Parlamento Europeo y del Consejo, de 9 de marzo de 1999, sobre equipos radioeléctricos y equipos terminales de telecomunicación y reconocimiento mutuo de su conformidad, Comunidades Europeas, Bruselas, documento 31999L0005. Disponible en:

https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A31999L0005
05/09/2018.

[11] ETSI EN 300 927 V5.4.1 (2000-12) "Digital cellular telecommunications system (Phase 2+); Numbering, addressing and identification (GSM 03.03 version 5.4.1 Release 1996)". Disponible en:

https://www.etsi.org/deliver/etsi_en/300900_300999/300927/05.04.01_60/en_300927v050401p.pdf 15/02/2018.

[12] ETSI EN 300 940 V7.7.1 (2000-10) "Digital cellular telecommunications system (Phase 2+); Mobile radio interface layer 3 specification (GSM 04.08 version 7.7.1 Release 1998)". Disponible en:

https://www.etsi.org/deliver/etsi_en/300900_300999/300940/07.07.01_60/en_300940v070701p.pdf 17/02/2018.

[13] ETSI TS 100 573 V8.4.0 (2000-07) "Digital cellular telecommunications system (Phase 2+); Physical layer on the radio path; General description (GSM 05.01 version 8.4.0 Release 1999)". Disponible en:

https://www.etsi.org/deliver/etsi_ts/100500_100599/100573/08.04.00_60/ts_100573v080400p.pdf 25/02/2018.

[14] ETSI EN 300 908 V8.5.1 (2000-11) "Digital cellular telecommunications system (Phase 2+); Multiplexing and multiple access on the radio path (GSM 05.02 version 8.5.1 Release 1999)". Disponible en:

https://www.etsi.org/deliver/etsi_en/300900_300999/300908/08.05.01_60/en_300908v080501p.pdf 04/03/2018.

[15] ETSI EN 300 909 V8.5.1 (2000-11) "Digital cellular telecommunications system (Phase 2+); Channel coding (GSM 05.03 version 8.5.1 Release 1999)". Disponible en:

https://www.etsi.org/deliver/etsi_en/300900_300999/300909/08.05.01_60/en_300909v080501p.pdf 15/03/2018.

[16] ETSI EN 300 959 V7.1.1 (2000-06) "Digital cellular telecommunications system (Phase 2+); Modulation (GSM 05.04 version 7.1.1 Release 1998)". Disponible en:

https://www.etsi.org/deliver/etsi_en/300900_300999/300959/07.01.01_60/en_300959v070101p.pdf 17/03/2018.

[17] Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, Jefatura del Estado, España, BOE-A-2003-20253 Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2003-20253

ANEXO A. LISTA DE ACRÓNIMOS

- MSK: Minimum Shift Keying
- GMSK: Gaussian minimum shift keying
- GSM: Global System for Mobile communications
- IEEE Institute of Electrical and Electronics Engineers
- MTS: Mobile Telephone System
- PSK: Phase Shift Keying
- EDGE: Enhanced Data Rates for GSM Evolution
- QAM: Quadrature Amplitude Modulation
- UMTS: Universal Mobile Telecommunications System
- LTE: Long Term Evolution
- IFFT: Inverse Fast Fourier Transform
- FDMA: Frequency Division Multiple Access
- TDMA: Time Division Multiple Access
- SDMA: Space Division Multiple Access
- CDMA: Code Division Multiple Access
- HSDPA: High Speed Downlink Packet Access
- HSUPA: High Speed Uplink Packet Access
- HSPA: High Speed Packet Access
- OFDMA: Orthogonal FDMA
- UL: Uplink
- DL: Downlink
- SCH: Synchronization Channel
- RACH: Random Access Channel
-TCH: Traffic Channels
-BCH: Broadcast Channels
-BCCH: Broadcast Control Channel
-FCCH: Frequency Control Channel
-DCCH: Dedicated Control Channels
-SACCH: Slow Associated Control Channel
-FACCH: Fast Associated Control Channel
-SDCCH: Stand-Alone Dedicated Control Channel
-CCCH: Common Control Channels
-PCH: Paging Channel
-AGCH: Access-Grant Channel

- SDR: Sofwtare Defined Radio
- ADC: Analogic to Digital Converter
- DAC: Digital to Analogic Converter
-AMPS: Advanced Mobile Phone System
- NTT: Nippon Denshin Denwa Kabushiki-gaisha
- AT&T: American Telephone and Telegraph
-CEPT: Committee of European Postal & Telephone
- NSS: Network Switching Subsystem
-MSC: mobile switching central
-BTS: Base Transceiver Station
-BSC: base station controller
-SIM: Subscriber Identity Module
-AUC: Authentication Centre
-HLR: Home Location Register
-VLR: Visitor Location Register
-EIR: Equipment Identity Register
-IMEI: International Mobile Station Equipment Identity
-W – CDMA: Wideband Code División Multiple Access
-ITU: International Telecommunication Union
-3GPP: 3rd Generation Partnership Project
-EV – DO: Evolution – Data Optimized
-MIMO: Multiple-input Multiple-output
-OWA: Open Wireless Architecture
-OTP: Open Transport Protocol
-SIR: Signal Interference Ratio

ANEXO B. SUMMARY.

In this project we will inhibit the communications network of the second generation GSM. The method described above is a method that stands out for its efficiency in terms of power.

We understand by a frequency inhibitor a device capable of hindering or preventing radiofrequency communications in a certain spectrum among communications devices that are in it's scope, but, Exactly how does this work?

A frequency inhibitor consists of a wave generator and a transmitter, whose objective is not to eliminate or suppress certain frequencies of the spectrum, it's to produce a sufficiently strong noise that makes it impossible for the transmitter and the receiver to establish a communication. For this, the wave generator through a signal without useful information (noise) that the transmitter emits at a higher power than the system to interfere, thus making the information transmitted by the system completely useless.

The need for the existence of these devices is due to the wide use that is being given progressively to the radio spectrum and communications. As expected, there are people who are capable of giving these communication technologies a negative or terrorist use. A clear example is the bombs by remote control, it's not even necessary to be in a place to blow up a bomb, it's enough to send a radio signal to it to order it to explode. An other example is to maintain some secret place safe of any signal. The fact is that there are very dangerous uses that can be given to telecommunication technologies by nobody and for this reason it is sometimes convenient to interfere with these signals.

Another typically military necessity for the existence of frequency inhibitors is their ability to avoid enemy communications, one of the key historical objectives for victory is to leave the soldiers off from their generals and leaders. But this does not only affect the war on the ground, without going further than a simple microphone that is in our house or any room is capable of violating our freedom. A striking example is the Russian microphone that was introduced into the American embassy in Russia during the Cold War. This device emitted radio waves to transmit what was said in the room and was not detected because it was passive, that's it, it did not need an external power source. This microphone was operational for about 5 years.

This type of situation would have been avoided with a simple inhibitor, that although there was more than one microphone listening, the information could not be transmitted. Therefore inhibitors are a technology that was doomed to be created by necessity, because of the technological increase that radiocommunications are suffering.

Like all new technology, it is not absent that somebody can use it inappropriately, for example, a frequency inhibitor can be used to prevent communications between authorities or private persons, as well as to circumvent security systems that use the radio spectrum to communicate a fault or a video signal.

These cases are also a reason why the use of frequency inhibitors is entirely reserved for the security forces of the state and the army to provide protection to institutions, cars, official organisms and other sites that might be the target of a terrorist attack.

Frequency inhibitors are subject to regulations and laws to control their use by competent bodies such as the Agencia Estatal de Radiocomunicaciones, el Ministerio de Ciencia y Tecnología o la Comisión del Mercado de las Telecomunicaciones. The

breach of these laws will result in an economic penalty that could rise according to the impact generated from 30 thousand euros to 20 million euros.

The communications, have suffered a high evolution since it's creation. Today there are five generations of mobile telephony and each of them reflects an increase in user experience in terms of security, quality of service and speed. The network that we are going to try to inhibit belongs to the second generation and is the GSM network.

In the 1990s, GSM (Global System for Mobile communications) was born in the CEPT (Committee of European Postal & Telephone) telecommunications conference. It is a European standard that had the great advantage of digital communications.

The difference between digital and analog communications lies in the fact that digital communications provide a higher quality of service both in the quality of the call and in the security of information, since the call data is encrypted, in addition to digital technology it makes the size of the terminal much smaller by providing a smaller and more manageable mobile phones.

GSM has 200 kHz channels. Each channel has a capacity of 270,833 kbps and for data a maximum of 9.6 kbps in a channel, this is one of the main reasons why it is passed to the third generation as multimedia applications began to need higher speed. Maximum transmission power of the 2W terminal that drops to 1W in the GSM 1800MHz, 1900MHz band.

GSM appeared in Europe in the 900 MHz band and 1800 MHz, whereas in the United States in the 1900 MHz band, the reason for this was purely for legal reasons and the availability of unassigned frequencies

GSM works by circuit switching and access to the medium is done with TDMA although FDMA can also be used, complementing it with a channel change according to the needs of the network called frequency hopping. CDMA can also be used but this time the channel width is increased to 1.23 MHz. Among the services offered are:

• Digital voice.

• SMS.

• International roaming.

• Call waiting, call blocking and call retention.

For all these reasons, the GSM network is considered the first functional digital mobile network.

The GSM network works with cellular technology, it is formed by several base stations, each one of them consists of an antenna with a radius of coverage, this radius being the cell size. A base station can reach different coverage radios because in this case the radius needed in rural areas is different from that of the cities, of course because the number of users depends on the bandwidth and in the cities more base stations will be needed. Few hundred meters of radio because the cities have many users in a small space, while the rural areas have few users in a lot of space and here the base stations can reach a radius of 35 km.

The GSM network uses TDMA for greater efficiency, so the terminal is not transmitting the entire and saves the battery. In GSM the time is divided into slots of 576.9 μs, the first one is reserved for synchronization, by the base station for the DL and another slot to receive, the rest of the slots are free for the users. This allows a good use of the available spectrum and a longer duration of the battery when transmitting the terminal only the fractions of time that belong to it.

The base stations connected to a base station controller (BSC) which manages the resources provided to the base stations in terms of frequency distribution and power control.

The BSC is also responsible for not cutting communication when changing cell, this is done because the base stations measure the power which they receive a terminal and send this data to the BSC so it can triangulate where the terminal is located and deduce how it moves, therefore when the BSC observes that a terminal is going to pass from one cell to another it notifies the mobile switching center (MSC) to which it's physically connected and the terminal to make the jump. This process is known as handover or handoff and can also be when the base station closest to the terminal is saturated and connects to the next closest station or most powerfull. The MSC belongs to the network switching subsystem (NSS) which manages the identities of the users, location and establishment of communications with other users.

The MSC manages all this by connecting to databases such as the home location register (HLR), it's a database that contains information about location of registered users within the MSC area, each network must have at least an HLR. It also connects to the visitor location register (VLR), this database contains information of users who are not local subscribers to the MSC of a region, it's certainly a guest registry. The VLR collects the data of a visitor from the HLR and maintains it until the visitor leaves the MSC area in which he or she is, or after a period of inactivity.

Other records to which the MSC connects are the equipment identification record (EIR), which stores the IMEIs, a 15-digit number that is used by the EIR to generate white or black lists in order to reduce the odds of terminal theft or fraud. It also contains the list of mobile terminals and the authentication center (AUC) that is responsible for verifying the identities of the users, is associated with the HLR and contains the identification keys of the users, a 128-bit secret key (SIM) that it does not leave the AUC and a set of three keys is known as the authentication triplet.

The modulation used by GSM is a GMSK, this is a variant of the MSK modulation (Minimum-shift keying), we will explain this modulation first.

The MSK modulation is a continuous frequency shift modulation, coded with alternating bits between the quadrature components where the "aQ" component is delayed by half of the symbol period coded with each bit as a sinusoidal mean giving rise to a constant envelope signal which reduces the problems of non-linear distortion. In the MSK the difference between the lower and upper frequency is exactly half the bit rate, so the maximum frequency deviation is 25% of the maximum modulation frequency, therefore the modulation index is 0.5, which causes that the waves to represent a zero and a one are orthogonal. Next, the mathematical expression of the MSK.

$$s(t) = a_I(t)\ \cos\frac{\pi t}{2T}\ \cos 2\pi f_c t - \ a_Q(t)\ \sin\frac{\pi t}{2T}\ \sin 2\pi f_c t \qquad \text{(B.1)}$$

GSM uses various types of channels, traffic channels (TCH), control channels, where there are diffusion (FCCH, SCH, BCCH), common (CCCH, RACH, PCH, AGCH) and dedicated (SADCCH, SACCH, FACCH). But we are going to focus on the diffusion control channels because these are the means by which the base station manages to synchronize the mobile terminal, they all go through the downlink.

When the mobile terminal is turned on, it's tuned in frequency and time, then decodes the BCCH channels and checks if the SIM is valid in the network, the location is updated and authenticated.

The FCCH channel is used for the frequency synchronization of the base station with the mobile terminal, consisting of a burst of zeros modulated with a GMSK that produces a continuous sinusoidal signal that serves to show the mobile terminal at the frequency to which it has to synchronize.

The SCH, once the mobile terminal is synchronized in frequency to the base station, synchronized in time is needed. The SCH carries in it the number of the frame and the BSIC which is the identity code of the base station, which indicates to which base station the mobile terminal is connecting. The SCH channel is composed of 25 bits of information divided into 19 bits for the reduced frame number, 6 bits for the BSIC, 3 bits for the BCC which is the color code of the base station and another 3 bits for the NCC which is the color code of the network.

The BCCH channel what it does is send signaling information to all the terminals of the cell segregated in small messages called system messages, to take all the complete information, 4 consecutive BCCHs are needed in the first interval of the multi - frame 51, although if necessary, they can also be sent in the following intervals.

Among the information contained in the BCCH is:

• Identity of the GSM network.

• Frequencies used in the cell and neighboring cells.

• Information of the VLR.

• Maximum power to use in the control channels.

• Maximum number of control channel repetitions.

• Number of time slots for paging and assignment.

The base station continuously transmits system messages which help the mobile terminals to determine whether or not they can connect to the cell, some of these messages are mandatory and others optional and some have to be transmitted by the SACCH.

All these channels go in what is known as multi - frame 51. It is a multi - frame of 51 slots in which each slot contains the channel 's frame and in which it is clearly observed how TDMA is used in GSM. Hierarchically there is another multi - frame of 27 frames which is used for traffic and associated control channels and these two in turn are collected in super - frames and hyperframes reaching a total of 2047 frames, but we are going to focus in the multi - frame of 51 frames because it's the one that contains the diffusion control channels that we will use to inhibit.

Well, our goal is to prevent the mobile terminal from correctly distinguishing the channels FCCH, BCCH or SCH, when one of these channels is not reachable, the mobile terminal will be unable to connect to the GSM network.

The main idea of our inhibition is to create a false FCCH channel which we have called interfering FCCH. This interfering FCCH does not contain useful information, on the contrary it only has noise. The fact of choosing this method is that since the FCCH is a sequence of zeros modulated with a GMSK, it makes its imitation and its transmission in terms of power very simple.

Once we have created our interfered FCCH with a GMSK, we have to send it sequentially every x time, I mean, we do not know the exact moment in which the base station starts transmitting to our mobile terminal to be synchronized, so we have to think of a way that our interfering FCCHs coincide in some way during the time in which the mobile terminal is trying to synchronize. To do this, I will show that the most effective is to send our interfering FCCH every two slots, so that at some point it will always coincide with more than one element of the multi - frame 51.

When our FCCH matches elements of the multi - frame 51 it makes them illegible. The great advantage of inhibiting with an interfering FCCH is that two forms of inhibition can happen, either the mobile terminal when encountering our interfering FCCH is obviously synchronized with erroneous data or it receives our interfering FCCH at the same time with other data and does not it is synchronized with none.

As in any inhibition the difference is in how much power is used to inhibit, this technique is very efficient in power since we do not transmit continuously and only need to transmit a little over the power with which the mobile terminal receives the base station.

Now I will demonstrate the most efficient relation in terms of the nominal power of the interfering FCCH and the number of interfering FCCHs that we are going to send.

First we are going to simulate an emitter which sends the modulated multi - frame 51 and a receiver that demodulates and receives it. For this the sequence logic that we have followed has been as follows: Generate the lowest level frames (the 156 bits) of the FCCH, BCCH, SCH and CCCH, then modulate them with a GMSK and mount them in the multi - frame 51, simulate that it is sent to the receiver and it separates the multi-frame 51 and demodulates the different channels.

When we already have all the modulated channels, what we have to do now is to build the multi - frame 51 since it is the one on which we are going to do the inhibition tests, simulating that the constructed multi - frame 51 is the one sent by the station base.

The next step is to find the best relationship between the potential size of our interfering FCCH and the number of them that we have to send.

The purpose of this is to calculate the error between the interference of the interfering FCCH and the normal FCCH as a function of the SIR to find the most favorable power ratio. In communications, a 10% error is considered sufficient to consider inhibition. To perform these calculations, it is sufficient to calculate in a loop the errors of the different interfering FCCHs superimposed on the normal FCCH

Once the power size of the interfering FCCH is established with respect to the normal FCCH, it is necessary to test the number of interfering FCCHs is the most efficient and in which part of the multi-frame 51. For this we have developed a program that calculates bit by bit the error of an interfering FCCH with 1.34 times the power of the normal FCCH superimposed on all the slots, then the same with two interfering FFCHs and then with three and go on until reaching a size of 0.17 times the size of the multi-frame 51 .

The 0.17 number is obtained by compare the resulting error based on the number of interfering FCCHs that we use, since we can not be emitting interfering FCCHs all the time that the multi - frame 51 lasts because it would produce a lot of power expenditure, we have decided to transmit as much as 17% of the time, that's it, about 40 ms. In the following figure we observe that the graph is ascending as expected since the more interfering FCCHs, the greater the error we will obtain. 17% is in 27 frames since 27 is 17% of 156.

With all these data it is concluded that the most efficient way to inhibit is to send a sequence of 27 interfering FCCHs at a power 1.34 times greater than the mobile terminal receives from the base station.

To translate this into practice we need the following tools:

• National Instruments USRP 2920.

• Vector analyzer.

• A computer, in this case mine: Sony Vaio SVE series.

• Software: Lab View student edition.

• 1 Gb Ethernet cable.

• Transmission antenna.

• USRP2920 charger.

Once we have all the tools we proceed to inhibit. To inhibit connect the antenna to USRP 2920 and this to the power supply network with the charger, we connect the USPR 2920 to the computer through the 1 Gb Ethernet cable and through Lab View we emit our interfering sequence which is collected by the vector analyzer. With the vector analyzer we are able to see in time and frequency the GSM frames that are transmitted and therefore to see if we inhibit correctly we have to observe distortion in said frames.

Another more effective way to know if we are inhibiting is to make use of a GSM telephone (2G) and knowing the frequency that the operator of the phone operates in GSM can inhibit the same frequency so that it is observed that effectively the mobile phone is unable to connect to the network.

To achieve this in Lab View we have had to develop a circuit model that is capable of sending this interfering sequence.

In the first instance, we developed the GMSK modulation circuit to be able to modulate our interfering FCCH, for this we have used a Gaussian filter and an MSK.

On the other hand we can start using the vector analyzer to observe the GMS network, its constellation and its frames. For them we configure the vector analyzer as a digital demodulator for the GSM network and we look for the frequencies in which this network is used.

The next step of the vector analyzer will be to observe the inhibition on the part of our inhibitor, so for the moment we leave it. Right now we have the vector analyzer ready and our interfering FCCH too, it just remains to create a frame of size 3 slots. We want to do this because as we said before in simulation, what we want is to send the interfering FCCH but not continuously in all the slots of the multi - frame 51 since that would be a very high power expenditure. What we will do then is build the 3-slot plot so that we will have them placed in the following way: Interfering FCCH, empty slot, empty slot. In this way if we send this frame continuously during the time calculated in

the simulations (40 ms of inhibition for each multi - frame 51) we will obtain our complete interferent frame, of course we will have to send several interfering sequences since the base station does not send a single multi - frame51.

Well, once we have everything we just have to inhibit, for that we run our program to emit the interfering sequence. To observe the inhibition we will use my phone, we will force it to work in the 2G network, GSM. This can be done easily from the phone settings.

To know if we are inhibiting or have not we have downloaded an application that allows us details about the CID of the base station from which we are connected and we got the 5441 CID.

Unfortunately, no application has been able to show us the frequency in which this BTS transmits so we have had to try to inhibit all the GSM frequencies of Movistar until we find the frequency at which the station transmits. As a result we have found the frequency of 935.8 MHz.

In this frequency we have managed to inhibit the base station of CID 5541 to stop serving us, as a result the phone jumps to another base station with other frequency. We have verified that when the phone starts to search a network again and to stop the inhibitor, the telephone reconnects to the base station of CID 5541 and if we re-activate the inhibitor it loses its signal again and skips frequency.

We have checked the operation of the inhibitor for different frames at different powers. In the first case, we tried to continuously transmit an interfering FCCH, with the minimum power required to inhibit 25 dB. In the second case we have tried to inhibit with a sequence like the one we have generated in the theory, in this case we have not managed to inhibit rather if we use the maximum of the power that the USRP 2920 allows, which is 31 dB. In view of this, we have decided to increase the presence of the interfering FCCH and in this third case we send for each empty slot, two interfering FCCHs (before it was the other way) and now we have managed to inhibit up to a minimum of 27 dB of gain.

The social impact of this technology is both positive and negative in aspects of safety and health, of course positive economically speaking since all technology produces money and ultimately negative in terms of freedom because our ability to connect can be see altered without need or know that we are facing a frequency inhibitor.

In 2017, mobile telephony technologies and services generated 4.5% of the world's GDP, a valuation of 3.6 billion dollars. Around 29 million jobs have been generated directly or indirectly throughout the world and has enriched the public sector by 500 billion dollars in taxes and through radio spectrum auctions.

Like any new technology that arises, there are these inhibitors and anti inhibitors that leads the humans being in the future to develop inhibitors and ant inhibitors much more sophisticated. The life cycle of technology consists in feeding on itself to continue evolving.